Appliance Dell DL4000
Guía del usuario

Notas, precauciones y avisos

NOTA: Una NOTA proporciona información importante que le ayuda a utilizar mejor su equipo.

PRECAUCIÓN: Una PRECAUCIÓN indica la posibilidad de daños en el hardware o la pérdida de datos, y le explica cómo evitar el problema.

AVISO: Un mensaje de AVISO indica el riesgo de daños materiales, lesiones corporales o incluso la muerte.

Copyright © 2014 Dell Inc. Todos los derechos reservados. Este producto está protegido por leyes internacionales y de los Estados Unidos sobre los derechos de autor y la protección intelectual. Dell™ y el logotipo de Dell son marcas comerciales de Dell Inc. en los Estados Unidos y en otras jurisdicciones. El resto de marcas y nombres que se mencionan en este documento, puede ser marcas comerciales de las compañías respectivas.

2014 - 10

Rev. A04

Tabla de contenido

1 Introducción al appliance Dell DL4000 11

Acerca de su appliance DL4000 11
Tecnologías de Core DL4000 11
Live Recovery 11
Recuperación comprobada 11
Universal Recovery 12
Desduplicación global real 12
Arquitectura True Scale 12
Arquitectura de Implementación 13
Smart Agent 15
DL4000 Core 15
Proceso de instantáneas 15
Sitio de recuperación de desastres de replicación o proveedor de servicio 16
Recuperación 16
Características del producto 16
Repository (Repositorio) 17
Desduplicación global real 17
Cifrado 18
Replicación 19
Recuperación como servicio (RaaS) 20
Retención y archivado 20
Virtualización y nube 21
Administración de alertas y eventos 22
Portal de licencias 22
Consola web 22
API de administración de servicios 22

2 Trabajar con DL4000 Core 23

Acceso a la DL4000 Core Console 23
Actualización de los sitios de confianza en Internet Explorer 23
Configuración de exploradores para acceder de manera remota a Core Console 23
Planificación de la configuración del Core 24
Administración de licencias 25
Cambio de una clave de licencia 25
Cómo ponerse en contacto con el servidor del portal de licencias 25
Administración de la configuración del Core 26
Cómo cambiar el nombre de visualización del Core 26
Ajuste de la hora de los trabajos nocturnos 26

Modificación de la configuración de la cola de transferencias 27
Ajuste de la configuración del tiempo de espera del cliente 27
Configuración de los valores de caché de la desduplicación 28
Modificación de la configuración del motor 28
Modificación de la configuración de la conexión con la base de datos 29
Acerca de los repositorios 30
Plan para administrar un repositorio 31
Creación de un repositorio 32
Visualización de los detalles de un repositorio 35
Modificación de la configuración del repositorio 35
Ampliación de un repositorio existente 36
Cómo agregar una ubicación de almacenamiento a un repositorio existente 36
Comprobación de un repositorio 38
Eliminación de un repositorio 39
Cómo volver a montar volúmenes 39
Recuperación de un repositorio 39
Administración de la seguridad 40
Cómo agregar una clave de cifrado 40
Edición de una clave de cifrado 41
Cómo cambiar la frase de contraseña de la clave de cifrado 41
Importación de una clave de cifrado 41
Exportación de una clave de cifrado 42
Eliminación de una clave de cifrado 42
Administración de cuentas de servicios en la nube 42
Cómo agregar una cuenta de servicios en la nube 42
Edición de una cuenta de servicios en la nube 44
Configuración de los valores de la cuenta de servicios en la nube 44
Comprensión de la replicación 45
Acerca de la protección de estaciones de trabajo y servidores 45
Acerca de la replicación 45
Acerca de la inicialización 47
Acerca de la conmutación por error y la conmutación por recuperación 48
Acerca de la replicación y los puntos de recuperación cifrados 48
Acerca de las políticas de retención para replicación 48
Consideraciones de rendimiento para la transferencia de datos replicados 48
Plan para realizar la replicación 49
Replicación a un Core administrado automáticamente 50
Replicación a un Core administrado por un tercero 54
Supervisión de la replicación 57
Administración de configuraciones de replicación 59
Eliminación de replicación 59
Eliminación de un Agent de la replicación en el Core de origen 60

Eliminación de un Agent en el Core de destino 60
Eliminación de un Core de destino de la replicación 60
Eliminación de un Core de origen de la replicación 60
Recuperación de datos replicados 61
Plan para la conmutación por error y la conmutación por recuperación 61
Configuración de un entorno para la conmutación por error 61
Cómo realizar una conmutación por error en el Core de destino 62
Cómo realizar una conmutación por recuperación 62
Administración de eventos 63
Configuración de grupos de notificación 64
Configuración de un servidor de correo electrónico y de una plantilla de notificaciones de correo electrónico 66
Configuración de la reducción de repeticiones 67
Configuración de la retención de eventos 67
Administración de la recuperación 67
Acerca de la información del sistema 68
Visualización de la información del sistema 68
Descarga de instaladores 68
Acerca del instalador Agent 68
Descarga e instalación del instalador Agent 69
Acerca de la Utilidad de montaje local 69
Descarga e instalación de la Local Mount Utility (Utilidad de montaje local) 69
Cómo agregar un Core a la Local Mount Utility (Utilidad de montaje local) 70
Montaje de un punto de recuperación mediante la Local Mount Utility (Utilidad de montaje local) 71
Exploración de un punto de recuperación montado mediante la Local Mount Utility (Utilidad de montaje local) 72
Desmontaje de un punto de recuperación mediante la Local Mount Utility (Utilidad de montaje local) 72
Acerca del menú de bandeja de la Local Mount Utility (Utilidad de montaje local) 73
Uso de las opciones de Core y Agent 73
Administración de políticas de retención 74
Archivado en una nube 74
Acerca del archivado 75
Creación de un archivo 75
Configuración del archivado programado 76
Pausa o Reanudación de un archivado programado 77
Edición de un archivado programado 78
Comprobación de un archivo 79
Importación de un archivo 79
Administración de la conectabilidad de SQL 80
Configuración de los valores de conectabilidad de SQL 80

Configuración nocturna de las comprobaciones de conectabilidad SQL y el truncamiento de registro 82
Administración de las comprobaciones de capacidad de montaje de la base de datos de Exchange y truncamiento de registro 82
Configuración de la capacidad de montaje de la base de datos de Exchange y truncamiento de registro 82
Cómo forzar una comprobación de la capacidad de montaje 83
Cómo forzar comprobaciones de suma de comprobación 83
Cómo forzar el truncamiento de registro 83
Indicadores de estado de punto de recuperación 84

3 Administración del appliance DL4000 86
Supervisión del estado del appliance DL4000 86
Aprovisionamiento de almacenamiento 86
Aprovisionamiento del almacenamiento seleccionado 88
Eliminación de asignación de espacio para un disco virtual 88
Resolución de tareas erróneas 89
Actualización del appliance DL4000 89
Reparación del appliance DL4000 89

4 Protección de estaciones de trabajo y servidores 91
Acerca de la protección de estaciones de trabajo y servidores 91
Configuración de los valores de la máquina 91
Visualización y modificación de los valores de configuración 91
Visualización de la información del sistema de una máquina 92
Configuración de grupos de notificación para eventos del sistema 93
Edición de los grupos de notificación para eventos del sistema 94
Personalización de la configuración de la política de retención 96
Visualización de la información de la licencia 99
Modificación de los programas de protección 99
Modificación de la configuración de las transferencias 100
Reinicio de un servicio 103
Visualización de los registros de la máquina 103
Cómo proteger una máquina 104
Implementación del software del Agent al proteger un Agent 106
Creación de programas personalizados para volúmenes 107
Modificación de la configuración de Exchange Server 107
Modificación de la configuración de SQL Server 108
Implementación de un Agent (Instalación de inserción) 108
Replicación de un Agent nuevo 109
Administración de las máquinas 111
Extracción de una máquina 111

Replicación de los datos de Agent en una máquina 111
Configuración de la prioridad de replicación para un Agent 112
Cancelación de operaciones en una máquina 112
Visualización del estado de la máquina y otros detalles 113
Administración de varias máquinas 114
Implementación en varias máquinas 114
Supervisión de la implementación de varias máquinas 119
Protección de varias máquinas 120
Supervisión de la protección de varias máquinas 121
Administración de instantáneas y puntos de recuperación 122
Visualización de puntos de recuperación 122
Visualización de un punto de recuperación específico 123
Montaje de un punto de recuperación para una máquina Windows 124
Desmontaje de puntos de recuperación seleccionados 125
Desmontaje de todos los puntos de recuperación 125
Montaje de un volumen de punto de recuperación en una máquina Linux 125
Eliminación de puntos de recuperación 126
Eliminación de una cadena de puntos de recuperación huérfanos 127
Cómo forzar una instantánea 127
Cómo pausar y reanudar la protección 128
Restablecimiento de datos 128
Acerca de la exportación de datos protegidos de máquinas de Windows a máquinas virtuales 128
Exportación de información de copia de seguridad de una máquina Windows a una máquina virtual 129
Exportación de datos de Windows mediante exportación ESXi 130
Exportación de datos de Windows mediante una exportación VMware Workstation 131
Exportación de datos de Windows mediante exportación Hyper-V 134
Cómo realizar una reversión 138
Cómo realizar una reversión para una máquina Linux mediante la línea de comandos 139
Acerca de la restauración desde cero para máquinas Windows 140
Requisitos previos para realizar una restauración completa para una máquina Windows 141
Plan para realizar una restauración desde cero para una máquina Windows 141
Creación de la imagen ISO de un CD de inicio 141
Cómo cargar un CD de inicio 143
Cómo iniciar una restauración desde el Core 144
Asignación de volúmenes 145
Visualización del progreso de la recuperación 145
Inicio de un servidor de destino restaurado 146
Reparación de problemas de inicio 146
Cómo realizar una restauración desde cero para una máquina Linux 146
Instalación de la utilidad de pantalla 148

Creación de particiones de inicio en una máquina Linux 148
Visualización de eventos y alertas 149

5 Protección de clústeres de servidor 150
Acerca de la protección de clúster de servidor 150
Aplicaciones admitidas y tipos de clúster 150
Protección de un clúster 151
Protección de nodos en un clúster 152
Proceso de modificación de la configuración del nodo de clúster 154
Plan para configurar los valores del clúster 154
Modificación de la configuración de clúster 154
Configuración de notificaciones de evento de clúster 155
Modificación de la política de retención de clúster 156
Modificación de los programas de protección de clúster 157
Modificación de la configuración de transferencia de clúster 157
Conversión de un nodo de clúster protegido en un Agent 158
Visualización de información del clúster del servidor 158
Visualización de información del sistema de clúster 158
Visualización de la información de resumen 159
Cómo trabajar con puntos de recuperación de clúster 159
Administración de instantáneas para un clúster 160
Cómo forzar una instantánea para un clúster 160
Cómo pausar y reanudar instantáneas de clúster 160
Cómo desmontar puntos de recuperación locales 161
Como realizar una reversión para clústeres y nodos de clúster 161
Cómo realizar una reversión para clústeres CCR (Exchange) y DAG 161
Cómo realizar una reversión para clústeres SCC (Exchange, SQL) 162
Replicación de datos de clúster 162
Eliminación de un clúster de la protección 162
Eliminación de nodos de clúster de la protección 163
Eliminación de todos los nodos de un clúster de la protección 163
Visualización de un informe de clúster o nodo 163

6 Emisión de informes 165
Acerca de los informes 165
Acerca de la barra de herramientas de informes 165
Acerca de los informes de cumplimiento 165
Acerca de los informes de errores 166
Acerca del informe de resumen del Core 166
Resumen de repositorios 166
Resumen de Agents 167
Cómo generar un informe para un Core o Agent 167

Acerca de los informes de Core de la Central Management Console (Consola de administración central) 168
Cómo generar un informe desde la Central Management Console (Consola de administración central) 168

7 Realizar una recuperación completa del appliance DL4000..... 169
Creación de una partición RAID 1 para el sistema operativo..... 169
Instalación del sistema operativo..... 170
Ejecución de la Recovery and Update Utility (Utilidad de actualización y recuperación)..... 171

8 Cómo cambiar el nombre del host manualmente..... 172
Detención del servicio de Core..... 172
Eliminación de certificados del servidor..... 172
Eliminación del servidor del Core y de las claves de registro..... 173
Inicio de Core con el nuevo nombre de host..... 173
Cómo cambiar el nombre de visualización 173
Actualización de los sitios de confianza en Internet Explorer..... 173

9 Apéndice A — Secuencias de comandos..... 175
Acerca de las secuencias de comandos de PowerShell 175
Requisitos previos para secuencias de comandos de PowerShell 175
Pruebas de secuencias de comandos 176
Parámetros de entrada 176
ChecksumCheckJobRequest (namespace Replay.Core.Contracts.Exchange.ChecksumChecks)DatabaseCheckJobRequestBase (namespace Replay.Core.Contracts.Exchange)ExportJobRequest (namespace Replay.Core.Contracts.Export) NightlyAttachabilityJobRequest (namespace Replay.Core.Contracts.Sql) RollupJobRequest (namespace Replay.Core.Contracts.Rollup) TakeSnapshotResponse (namespace Replay.Agent.Contracts.Transfer)TransferJobRequest (namespace Replay.Core.Contracts.Transfer) VolumeImageIdsCollection (namespace Replay.Core.Contracts.RecoveryPoints) VolumeNameCollection (namespace Replay.Common.Contracts.Metadata.Storage) VolumeSnapshotInfoDictionary (namespace Replay.Common.Contracts.Transfer) 178
Pretransferscript.ps1 182
Posttransferscript.ps1 183
Preexportscript.ps1 183
Postexportscript.ps1 184
Prenightlyjobscript.ps1 184
Postnightlyjobscript.ps1..... 186
Secuencias de comandos de ejemplo 188

10 Obtención de ayuda..... 189
Búsqueda de documentación..... 189
Búsqueda de actualizaciones de software..... 189
Cómo ponerse en contacto con Dell..... 189
Comentarios sobre la documentación..... 189

1

Introducción al appliance Dell DL4000

Este capítulo describe las características, la funcionalidad y la arquitectura de DL4000.

Acerca de su appliance DL4000

Dell DL4000 combina funciones de copia de seguridad y replicación en un producto unificado de protección de datos. Proporciona una recuperación fiable de los datos de aplicación a partir de sus copias de seguridad para proteger las máquinas virtuales y las máquinas físicas. Dell DL4000 es capaz de manejar petabytes de datos con desduplicación global, compresión, cifrado y replicación integrados en la infraestructura de nube privada o pública específica. Los datos y las aplicaciones de servidor se pueden recuperar en minutos con fines de retención de datos (DR) y cumplimiento.

DL4000 admite entornos de varios hipervisores en nubes públicas y privadas de VMware vSphere y Microsoft Hyper-V .

DL4000 combina las siguientes tecnologías:

- Live Recovery
- Recuperación verificada
- Universal Recovery
- Desduplicación global real

Tecnologías de Core DL4000

Live Recovery

Live Recovery es una tecnología de recuperación instantánea para VM o servidores. Facilita un acceso prácticamente continuo a volúmenes de datos en servidores virtuales o físicos. Puede recuperar un volumen completo con RTO próximo a cero y un RPO de minutos.

La tecnología de copia de seguridad y replicación registra instantáneas simultáneas de varias VM o servidores y proporciona protección del sistema y los datos de manera casi instantánea. Puede reanudar el uso del servidor directamente desde el archivo de copia de seguridad sin esperar a una restauración completa en el almacenamiento de producción.

Recuperación comprobada

La opción Verified Recovery (Recuperación comprobada) le permite realizar pruebas de recuperación automatizadas y comprobación de copias de seguridad. Incluye, pero sin limitarse a, sistemas de archivos, Microsoft Exchange 2007, 2010 y 2013, y versiones diferentes de Microsoft SQL Server 2005, 2008, 2008 R2, 2012 y 2014. La opción Verified Recovery (Recuperación comprobada) ofrece un 100% de capacidad de recuperación de aplicaciones y copias de seguridad en entornos virtuales y físicos. Incluye un algoritmo de comprobación de la integridad total basado en claves SHA de 256 bits que

comprueba la exactitud de cada bloque de disco de la copia de seguridad durante las operaciones de archivado, replicación e inicialización de los datos. Esto garantiza la pronta identificación de los datos dañados y evita que los bloques de datos dañados se conserven o transfieran durante el proceso de copia de seguridad.

Universal Recovery

La tecnología Universal Recovery le ofrece flexibilidad ilimitada para la restauración de máquinas. Puede restaurar sus copias de seguridad desde sistemas físicos a máquinas virtuales, máquinas virtuales a máquinas virtuales, máquinas virtuales a sistemas físicos o sistemas físicos a sistemas físicos y realizar restauraciones desde cero a hardware diferente, P2V, V2V, V2P, P2P, P2C, V2C, C2P y C2V.

La tecnología Universal Recovery también acelera los movimientos a plataformas diferentes entre máquinas virtuales. Por ejemplo, permite mover de VMware a Hyper-V o de Hyper-V a VMware. Crea recuperaciones a nivel de aplicación, a nivel de elemento y a nivel de objeto (archivos individuales, carpetas, correo electrónico, elementos de calendario, bases de datos y aplicaciones). Con AppAssure, puede recuperar o exportar de un medio físico o virtual a la nube.

Desduplicación global real

DL4000 proporciona True Global Deduplication (Desduplicación global real) que reduce considerablemente sus requisitos de capacidad de disco físico ofreciendo porcentajes de reducción de espacio que superan el 50%, al tiempo que sigue cumpliendo con los requisitos de almacenamiento de datos. La compresión y desduplicación de nivel de bloque en línea de AppAssure True Scale con rendimiento de velocidad de línea, así como la comprobación de integridad incorporada, evitan que los datos dañados afecten a la calidad de los procesos de copia de seguridad y archivado.

Arquitectura True Scale

DL4000 se basa en la arquitectura AppAssure True Scale. Aprovecha la arquitectura dinámica de conductos de varios Cores que se optimiza para ofrecer un potente rendimiento para sus entornos de empresa de forma constante. True Scale está diseñada desde la base para ser escalada linealmente y almacenar y administrar de forma eficaz grandes datos, así como para ofrecer RTO y RPO de minutos sin poner en peligro el rendimiento. Incluye un administrador de objetos y volúmenes incorporado para este fin con desduplicación, compresión, cifrado, replicación y retención globales integradas. El siguiente diagrama describe la arquitectura de AppAssure True Scale.

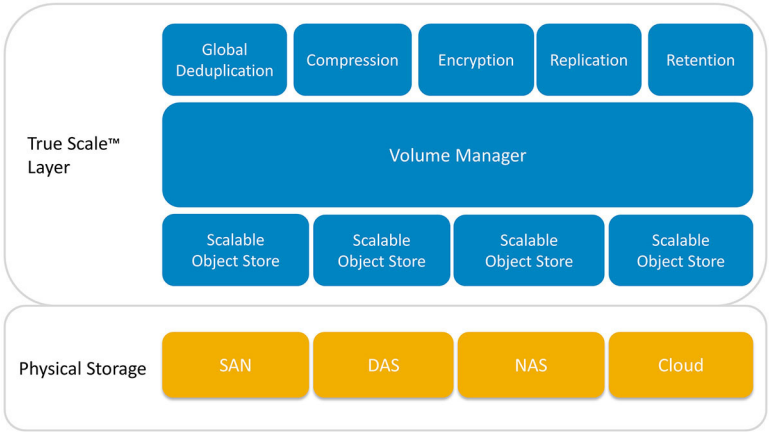

Ilustración 1. Arquitectura AppAssure True Scale

El administrador de volúmenes de AppAssure y el almacén de objetos escalable sirve como base de la arquitectura de AppAssure True Scale. El almacén de objetos escalable almacena instantáneas de nivel de bloque capturadas desde servidores virtuales y físicos. Los administradores de volúmenes administran los diversos almacenes de objetos ofreciendo un repositorio común o almacenamiento puntual solo para lo que sea necesario. El almacén de objetos admite simultáneamente todo, con E/S asíncrona que ofrece alto rendimiento con mínima latencia y maximiza el uso del sistema. El repositorio reside en diferentes tecnologías de almacenamiento como Storage Area Network (Red de área de almacenamiento - SAN), Direct Attached Storage (Almacenamiento conectado directamente - DAS) o Network Attached Storage (Almacenamiento conectado a la red - NAS).

La función del administrador de volúmenes de AppAssure es similar a la del administrador de volúmenes en un sistema operativo. Toma diversos dispositivos que pueden ser de distinto tamaño y tipo y los combina en volúmenes lógicos mediante políticas de asignación seccionada o secuencial. El almacén de objetos guarda, recupera, mantiene y, a continuación, replica objetos derivados de instantáneas que detectan aplicaciones. El administrador de volúmenes ofrece rendimiento de E/S escalable en combinación con administración de desduplicación, cifrado y retención de datos globales.

Arquitectura de Implementación

DL4000 es un producto de copia de seguridad y recuperación escalable que se implementa de forma flexible dentro de la empresa o como servicio ofrecido por un proveedor de servicio administrado. El tipo de implementación depende del tamaño y los requisitos del cliente. Preparar la implementación de DL4000 implica planificar la topología de almacenamiento de red, la infraestructura de hardware del Core y de recuperación de desastres y la seguridad.

La arquitectura de implementación se compone de componentes locales y remotos. Los componentes remotos pueden ser opcionales para los entornos que no necesiten usar un sitio de recuperación de desastres o un proveedor de servicio administrado para recuperación externa. Una implementación local básica se compone de un servidor de copia de seguridad denominado Core y una o más máquinas protegidas, conocidas como Agents. El componente externo se habilita mediante la replicación que ofrece capacidades de recuperación completas en el sitio de DR. El Core utiliza imágenes base e instantáneas incrementales para compilar los puntos de recuperación de los Agents protegidos.

Además, DL4000 reconoce aplicaciones porque detecta la presencia de Microsoft Exchange y SQL y de sus respectivas bases de datos y archivos de registro y, a continuación, agrupa automáticamente estos

volúmenes con dependencia para una protección global y una recuperación efectiva. Esto le garantiza que jamás tendrá copias de seguridad incompletas cuando esté realizando recuperaciones. Las copias de seguridad se realizan mediante instantáneas de nivel de bloque que reconocen aplicaciones. DL4000 también puede realizar truncamientos de registro de los servidores de Microsoft Exchange y SQL protegidos.

En el siguiente diagrama se representa una implementación sencilla. En este diagrama, los Agents se instalan en máquinas como un servidor de archivos, de correo electrónico, de bases de datos o en máquinas virtuales y se conectan y se protegen mediante un solo Core, que también incluye el repositorio central. El Portal de licencias administra las suscripciones de licencias, grupos y usuarios de los Agents y de los Cores de un entorno. El Portal de licencias permite a los usuarios iniciar sesión, activar cuentas, descargar software e implementar Agents y Cores en el entorno en función de su licencia.

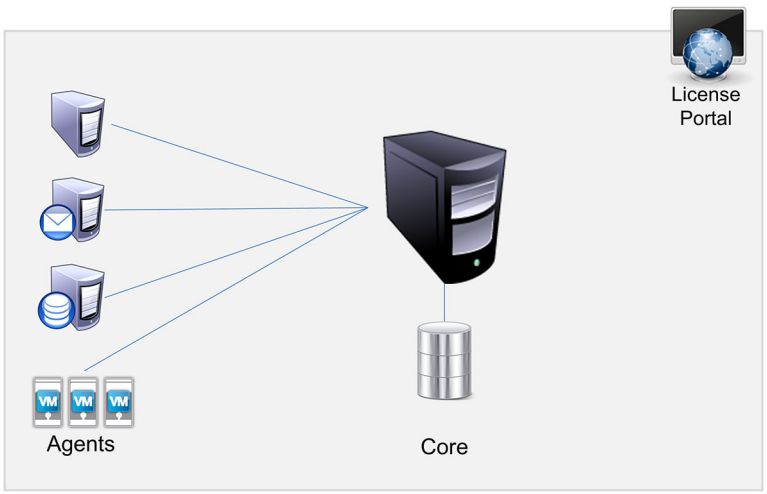

Ilustración 2. Arquitectura de implementación básica

También puede implementar varios Cores según se muestra en el siguiente diagrama. Una consola central administra varios Cores.

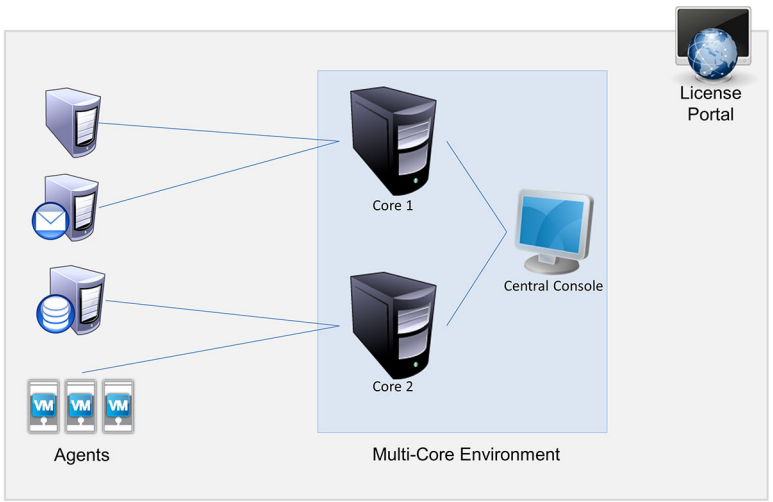

Ilustración 3. Arquitectura de implementación de varios Cores

Smart Agent

Smart Agent se instala en las máquinas protegidas por el Core. El Smart Agent hace un seguimiento de los bloques cambiados en el volumen de disco y, a continuación, captura una imagen de los bloques cambiados a un intervalo de protección predefinido. El enfoque continuo de las instantáneas de nivel de bloque incrementales evita que se repitan copias de los mismos datos de la máquina protegida en el Core. El Smart Agent reconoce las aplicaciones y está inactivo cuando no se usa, con un uso de la CPU de casi cero (0) y menos de 20 MB de sobrecarga de memoria. Cuando el Smart Agent está activo, hace un uso de la CPU de entre el 2% y el 4% y de menos de 150 MB de memoria, incluyendo la transferencia de instantáneas al Core. Esto es mucho menos que en los programas de software heredados, que usan niveles notablemente más altos de CPU y ancho de banda de memoria, aunque estén inactivos.

Smart Agent reconoce las aplicaciones porque detecta el tipo de aplicación que está instalada y también la ubicación de los datos. Automáticamente agrupa los volúmenes de datos con dependencia, caso de las bases de datos y luego los registra juntos para una protección eficaz y una recuperación rápida. Una vez configurado elAgent, utiliza tecnología inteligente para realizar un seguimiento de los bloques cambiados de los volúmenes de disco protegidos. Cuando la instantánea está lista, la transfiere rápidamente al Core usando conexiones basadas en sockets o multiproceso. Para conservar la memoria y el ancho de banda de la CPU en las máquinas protegidas, el Smart Agent no cifra ni desduplica los datos en el origen y las máquinas de Agent se emparejan con un Core para su protección.

DL4000 Core

DL4000 Core es el componente central de la arquitectura de implementación. El Core almacena y administra todas las copias de seguridad de la máquina y proporciona servicios de Core para copia de seguridad, recuperación y retención,replicación, archivado y administración. El Core es un equipo direccionable mediante red independiente que ejecuta una variante de 64 bits del sistema operativo Microsoft Windows. DL4000 realiza compresión en línea basada en destino, cifrado y desduplicación de datos de los datos recibidos del Agent. El Core almacena entonces las copias de seguridad de instantánea en un repositorio, que puede residir en diferentes tecnologías de almacenamiento, como por ejemplo Storage Area Network (Red de área de almacenamiento - SAN), Direct Attached Storage (Almacenamiento conectado directamente - DAS) o Network Attached Storage (Almacenamiento conectado a la red - NAS).

El repositorio también puede residir en almacenamiento interno del Core. El Core se administra accediendo a la siguiente URLdesde un explorador de web: **https://CORENAME:8006/apprecovery/admin**. Internamente, se puede acceder a todos los servicios de Core a través de las APIde REST. A los servicios de Core se puede acceder desde dentro del Core o directamente a través de Internet desde cualquier aplicación que pueda enviar una solicitud HTTP/HTTPS y recibir una respuesta HTTP/HTTPS. Todas las operaciones de API se realizan sobre SSL y se autentican mutuamente mediante certificados X.509 v3.

Los Cores se emparejan con otro Cores para la replicación.

Proceso de instantáneas

El proceso de protección comienza cuando una imagen base se transfiere de una máquina de Agent al Core, que es el único momento en el que se debe transportar una copia completa de la máquina por la red en condiciones de funcionamiento normales, seguida de instantáneas incrementales que se realizarán de manera permanente. El AppAssure Agent para Windows usa el Servicio de instantáneas de volumen de Microsoft (VSS) para detener y desactivar el vaciado de los datos de aplicación en un disco a

fin de capturar una copia de seguridad coherente con el sistema de archivos y con la aplicación. Cuando se crea una instantánea, el escritor de VSS en el servidor de destino evita que se escriba contenido en el disco. Durante el proceso de detención de escritura de contenido en disco, todas las operaciones de E/S del disco se ponen en cola y se reanudan solo después de completarse la instantánea, mientras finalizan todas las operaciones en curso y se cierran los archivos abiertos. El proceso de creación de una copia de instantánea no afecta significativamente al rendimiento del sistema de producción.

AppAssure usa Microsoft VSS porque cuenta con soporte integrado para todas las tecnologías internas de Windows, como NTFS, Registry o Active Directory, a fin de vaciar datos en el disco antes de la instantánea. Además, otras aplicaciones empresariales, como Microsoft Exchange y SQL, usan los complementos del escritor de VSS para que se le notifique cuándo se está preparando una instantánea y cuándo se deben vaciar las páginas de bases de datos usadas en el disco a fin de devolver la base de datos a un estado de transacción coherente. Es importante mencionar que VSS se usa para desactivar el vaciado de los datos de aplicaciones y del sistema en el disco, pero no para crear instantáneas. Los datos capturados se transfieren rápidamente y se almacenan en el Core. Al usar VSS para la creación de copias de seguridad, el servidor de aplicaciones no se presenta en modo de copia de seguridad durante un largo período de tiempo, ya que solo se tardan unos segundos en realizar la instantánea, en lugar de horas. Otra ventaja de utilizar VSS para las copias de seguridad es que permite que el Agent tome una instantánea de grandes volúmenes de datos a la vez, ya que la instantánea trabaja a nivel de volumen.

Sitio de recuperación de desastres de replicación o proveedor de servicio

El proceso de replicación requiere una relación de emparejamiento de origen-destino entre dos Cores. El Core de origen copia los puntos de recuperación de los Agents protegidos y, a continuación, los transmite de forma continua y asíncrona hasta el Core de destino en un sitio de recuperación de desastres remoto. La ubicación externa puede ser un centro de datos propiedad de la empresa (Core administrado automáticamente) o una ubicación o entorno de nube del proveedor de servicio (MSP) administrado por un tercero. Cuando replique a un MSP, puede usar flujos de trabajo integrados que le permiten solicitar conexiones y recibir notificaciones de comentarios automáticas. Para la transferencia de datos inicial, puede realizar la inicialización de datos mediante el uso de medios externos; esto es útil para conjuntos de datos o sitios grandes con enlaces lentos.

Si se produce una interrupción grave, DL4000 admite conmutación por error y conmutación por recuperación en entornos replicados. Si se produce una interrupción completa, el Core de destino en el sitio secundario puede recuperar instancias desde Agents replicados e iniciar inmediatamente la protección en las máquinas conmutadas por error. Después de restaurar el sitio primario, el Core replicado puede conmutar por recuperación los datos desde las instancias recuperadas de vuelta a Agents en el sitio primario.

Recuperación

La recuperación se puede realizar en el sitio local o en el sitio remoto replicado. Cuando la implementación esté en estado estable con protección local y replicación opcional, Core le permitirá realizar la recuperación mediante Verified Recovery, Universal Recovery, o Live Recovery.

Características del producto

Puede administrar la protección y recuperación de datos críticos mediante lo siguiente:

- Repository (Repositorio)
- Desduplicación global real

- Cifrado
- Replicación
- Recuperación como servicio (RaaS)
- Retención y archivado
- Virtualización y nube
- Administración de alertas y eventos
- Portal de licencias de AppAssure
- Consola web de Core
- API de administración de servicios

Repository (Repositorio)

El repositorio utiliza el Deduplication Volume Manager (Administrador de volúmenes de desduplicación - DVM) para implementar un administrador de volúmenes que proporciona compatibilidad para varios volúmenes, cada uno de los cuales podría residir en diferentes tecnologías de almacenamiento como Storage Area Network (Red de área de almacenamiento - SAN), Direct Attached Storage (Almacenamiento conectado directamente - DAS), Network Attached Storage (Almacenamiento conectado a la red - NAS) o el almacenamiento en nube. Cada volumen se compone de un almacén de objetos escalable con desduplicación. El almacén de objetos escalable se comporta como un sistema de archivos basado en registros, en el que la unidad de asignación de almacenamiento es un bloque de datos de tamaño fijo denominado registro. Esta arquitectura le permite configurar la compatibilidad de tamaño de bloques para compresión y desduplicación. Las operaciones de mantenimiento períodico se reducen a operaciones de metadatos desdes operaciones que hacen un uso intensivo del disco porque el mantenimiento períodico ya no mueve datos sino que solo mueve los registros.

El DVM puede combinar un conjunto de almacenes de objetos en un volumen que se pueden ampliar creando sistemas de archivos adicionales. Los archivos del almacén de objetos están preasignados y se pueden agregar a petición a medida que cambien los requisitos de almacenamiento. Es posible crear hasta 255 repositorios independientes en un único Core y posteriormente aumentar el tamaño de un repositorio agregando nuevas extensiones de archivo. Un repositorio ampliado puede contener hasta 4.096 extensiones que abarquen diferentes tecnologías de almacenamiento. El tamaño máximo de un repositorio es 32 exabytes. Puede haber varios repositorios en un único Core.

Desduplicación global real

La desduplicación global real es un método efectivo para disminuir las necesidades de almacenamiento de copias de seguridad mediante la eliminación de los datos redundantes o duplicados. Se trata de un método efectivo porque solo se almacena una instancia de los datos en varias copias de seguridad en el repositorio. Los datos redundantes se almacenan, aunque no físicamente; simplemente se reemplazan por un puntero a la única instancia de datos en el repositorio.

Las aplicaciones de copia de seguridad convencionales realizan copias de seguridad completas repetitivas todas las semanas. Sin embargo, el sistema DL4000 realiza copias del bloque incrementales de las máquinas de manera permanente. Este enfoque permanente incremental, combinado con la desduplicación de los datos, permite reducir drásticamente el volumen total de datos confirmados en el disco.

El diseño de disco convencional de un servidor consta de un sistema operativo, de aplicaciones y de datos. En la mayoría de los entornos, los administradores suelen usar un tipo habitual de sistema operativo de escritorio y de servidor en varios sistemas para una implementación y una administración efectivas. Cuando la copia de seguridad se realiza a nivel de bloque en varias máquinas al mismo tiempo,

se ofrece una vista más granular de lo que contiene la copia de seguridad y lo que no, con independencia del origen. Entre estos datos se incluye el sistema operativo, las aplicaciones y los datos de aplicaciones del entorno.

Ilustración 4. Diagrama de desduplicación

DL4000 realiza la desduplicación de datos en línea basada en destino, donde los datos de instantánea se transmiten al Core antes de que se desdupliquen. La desduplicación de datos en línea indica simplemente que los datos se desduplican antes de que se confirmen en el disco. Se trata de algo diferente a la desduplicación en origen o de posprocesamiento, donde los datos se desduplican en el origen antes de transferirse al destino para el almacenamiento, y en el posprocesamiento los datos se envían sin procesar al destino, donde se analizan y desduplican una vez confirmados en el disco. La desduplicación en origen consume muchos recursos del sistema de la máquina mientras que la desduplicación de datos de posprocesamiento necesita todos los datos requeridos en disco (una mayor sobrecarga de capacidad inicial) antes de comenzar el proceso de desduplicación. Por otro lado, la desduplicación de datos en línea no requiere capacidad de disco adicional ni ciclos de CPU en el origen o en el Core para el proceso de desduplicación. Por último, las aplicaciones de copia de seguridad convencionales realizan repetidas copias de seguridad completas cada semana, mientras que DL4000 realiza continuamente copias de seguridad de nivel de bloque de las máquinas. Este enfoque continuo incremental, en conjunto con la desduplicación de datos, ayuda a reducir de forma considerable la cantidad total de datos confirmados en el disco con una tasa de reducción 80:1.

Cifrado

DL4000 proporciona un cifrado integrado para proteger las copias de seguridad y los datos almacenados frente a un acceso o uso no autorizados, garantizando así la privacidad de los mismos. DL4000 ofrece un cifrado de alta seguridad, mediante el cual se prohíbe el acceso a las copias de seguridad de los equipos protegidos. Solo el usuario que disponga de la clave de cifrado podrá acceder y descifrar los datos. No existe límite en cuanto al número de claves de cifrado que se pueden crear y almacenar en un sistema. DVM usa un cifrado AES de 256 bits en el modo de Encadenamiento de bloques de cifrado (CBC) con

claves de 256 bits. El cifrado se realiza en línea en los datos de la instantánea, a velocidades de línea que no afectan al rendimiento. Esto se debe a que la implementación de DVM es multiproceso y usa una aceleración de hardware específica para el procesador en el que se implementa.

Además, el cifrado viene preparado para entornos con múltiples clientes. La desduplicación se ha limitado de manera específica a los registros cifrados con la misma clave; dos registros idénticos que se hayan cifrado con claves diferentes no se podrán desduplicar entre sí. Este diseño garantiza que no se pueda usar la desduplicación para revelar datos entre dominios de cifrado diferentes, lo que representa una ventaja para los proveedores de servicios administrados, ya que las copias de seguridad replicadas de varios inquilinos (clientes) se pueden almacenar en un solo Core sin que un inquilino vea o acceda a los datos de otro inquilino. Cada clave de cifrado de inquilino activo crea un dominio de cifrado dentro del repositorio en el que solo el propietario de las claves puede ver, acceder o usar los datos. En un entorno con múltiples clientes, los datos se particionan y desduplican dentro de los dominios de cifrado.

En escenarios de replicación, DL4000 utiliza SSL 3.0 para proteger las conexiones entre los dos Cores de una topología de replicación para impedir la intercepción furtiva y la manipulación.

Replicación

La replicación es el proceso de copiar puntos de recuperación y transmitirlos a una ubicación secundaria con el fin de la recuperación de desastres. El proceso requiere una relación de origen-destino emparejada entre dos Cores. La replicación se administra por máquina protegida, es decir, las instantáneas de copia de seguridad de una máquina protegida se replican en el Core de réplica de destino. Cuando la replicación está configurada, el Core de origen transmite de manera asíncrona y continua los datos de instantáneas incrementales al Core de destino. Puede configurar esta replicación de salida en el centro de datos propio de su compañía o en el sitio de recuperación de desastres remoto (es decir, un Core de destino administrado automáticamente) o en un proveedor de servicios administrado (MSP) que ofrezca servicios de recuperación de desastres y de copia de seguridad externos. Al realizar la replicación en un MSP, puede usar flujos de trabajo integrados que le permitan solicitar conexiones y recibir notificaciones de comentarios automáticas.

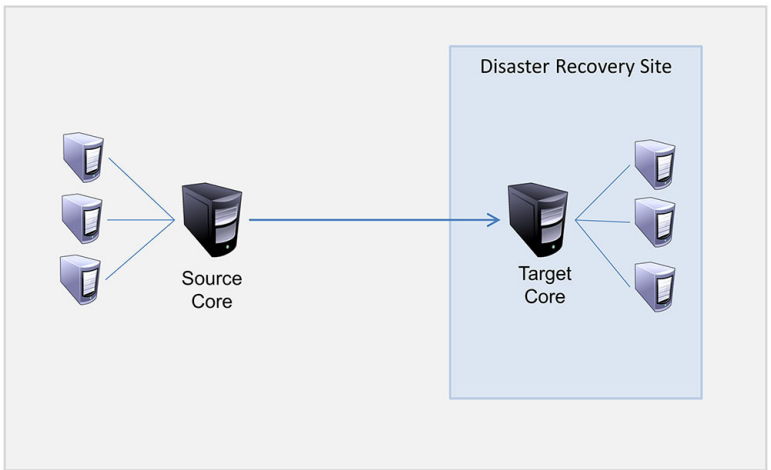

Ilustración 5. Arquitectura de replicación básica

La replicación se optimiza automáticamente con un algoritmo de lectura-coincidencia-escritura (RMW) que está estrechamente acoplado con la desduplicación. Con la replicación RMW, el servicio de

replicación de origen y de destino hace coincidir las claves antes de transferir los datos y, a continuación, replica sólo los datos comprimidos, cifrados y desduplicados de la WAN, haciendo que se reduzcan 10 veces los requisitos de ancho de banda.

La replicación comienza con la inicialización, la transferencia inicial de imágenes base desduplicadas e instantáneas incrementales de los Agents protegidos, que pueden sumar cientos o miles de gigabytes de datos. La replicación inicial se puede inicializar en el Core de destino mediante el uso de medios externos. Esto resulta normalmente útil para grandes conjuntos de datos o sitios con enlaces lentos. Los datos del archivo de inicialización se comprimen, cifran y desduplican. Si el tamaño total del archivo es mayor que el espacio disponible en el medio extraíble, el archivo podrá abarcar varios dispositivos, en función del espacio disponible en el medio. Durante el proceso de inicialización, los puntos de recuperación incrementales se replican en el sitio de destino. Después de que el Core de destino consuma el archivo de inicialización, los puntos de recuperación incrementales recién replicados se sincronizan de forma automática.

Recuperación como servicio (RaaS)

Los Managed Service Providers (Proveedores de servicios administrados - MSP) pueden aprovechar todas las ventajas de DL4000 como plataforma para proporcionar recuperación como servicio (RaaS). RaaS facilita recuperación en la nube completa al replicar los servidores físicos y virtuales de los clientes junto con sus datos en la nube del proveedor de servicio como máquinas virtuales, para permitir realizar operaciones de prueba de recuperación o de recuperación real. Los clientes que deseen realizar recuperación en la nube pueden configurar la replicación en sus máquinas protegidas en los Cores locales en un proveedor de servicio AppAssure. En caso de desastre, los MSP pueden conseguir que las máquinas virtuales adquieran velocidad nominal de rotación instantáneamente para el cliente.

Los MSP pueden implementar infraestructura RaaS basada en AppAssure, con múltiples clientes, que puede alojar organizaciones múltiples y discretas o unidades de negocio (los clientes) que normalmente no comparten seguridad o datos en un servidor único o en un grupo de servidores. Los datos de cada cliente se aíslan y protegen del resto de clientes y del proveedor de servicio.

Retención y archivado

En DL4000, las políticas de copia de seguridad y retención son flexibles y, por tanto, fácilmente configurables. La capacidad de adaptar las políticas de retención a las necesidades de una organización no solo ayuda a cumplir los requisitos de cumplimiento sino que lo hace sin poner en peligro los RTO.

Las políticas de retención se ejecutan los períodos durante los cuales las copias de seguridad se almacenan en medios a corto plazo (rápidos y caros). A veces, determinados requisitos empresariales y técnicos exigen ampliar la retención de estas copias de seguridad, pero el uso de almacenamiento rápido resulta inasequible. Por tanto, este requisito crea una necesidad de almacenamiento a largo plazo (lento y barato). Las empresas a menudo utilizan el almacenamiento a largo plazo para archivar tanto datos de cumplimiento como de no cumplimiento. La función de archivo se utiliza para admitir retenciones ampliadas de datos de cumplimiento y de no cumplimiento, y también se utiliza para inicializar los datos de replicación en un Core de destino.

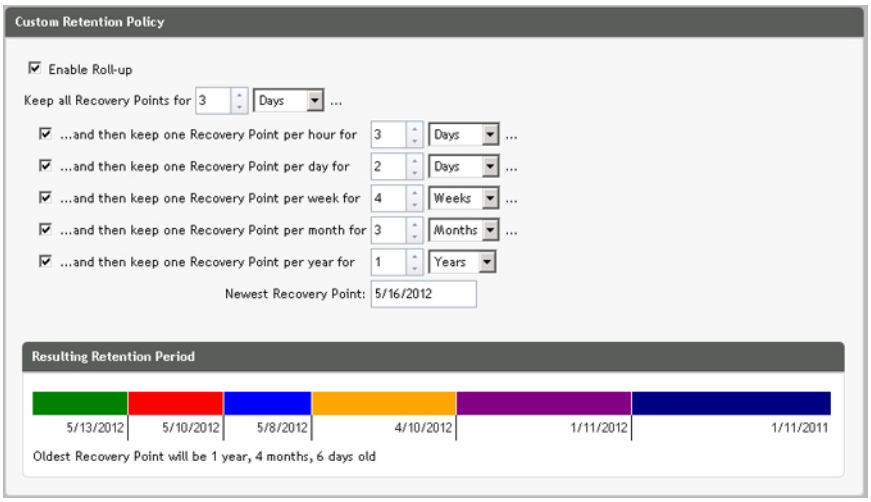
Custom Retention Policy
Enable Roll-up
Keep all Recovery Points for 3 Days ...
...and then keep one Recovery Point per hour for 3 Days ...
...and then keep one Recovery Point per day for 2 Days ...
...and then keep one Recovery Point per week for 4 Weeks ...
...and then keep one Recovery Point per month for 3 Months ...
...and then keep one Recovery Point per year for 1 Years
Newest Recovery Point: 5/16/2012
Resulting Retention Period
5/13/2012
5/10/2012
5/8/2012
4/10/2012
1/11/2012
1/11/2011
Oldest Recovery Point will be 1 year, 4 months, 6 days old

Ilustración 6. Custom Retention Policy (Política de retención personalizada)

En DL4000 las políticas de retención se pueden personalizar para especificar la duración de tiempo que se mantiene un punto de recuperación de copia de seguridad. Cuando la antigüedad de los puntos de recuperación se acerca al final de su período de retención, se quedan obsoletos y se quitan finalmente de la agrupación de retención. Normalmente, este proceso resulta ineficaz y acaba fallando, ya que la cantidad de datos y el período de retención empiezan a aumentar rápidamente. DL4000 resuelve este problema de grandes datos administrando la retención de grandes cantidades de datos con políticas de retención complejas y realizando operaciones de mantenimiento periódico para datos con antigüedad mediante operaciones de metadatos eficaces.

Las copias de seguridad se pueden realizar con un intervalo de algunos minutos y a medida que estas copias de seguridad vayan envejeciendo a lo largo de los días, los meses y los años. Las políticas de retención administran el envejecimiento y la eliminación de las copias de seguridad antiguas. Un método de organización lineal simple define el proceso de antigüedad. Los niveles de organización lineal se definen en minutos, horas y días;semanas, meses y años. La política de retención es aplicada por el proceso de mantenimiento periódico nocturno.

Para el archivado a largo plazo, DL4000 ofrece la posibilidad de crear un archivo del Core de origen y de destino en cualquier medio extraíble. El archivo se optimiza internamente y todos los datos del archivo se comprimen, cifran y desduplican. Si el tamaño total del archivo es superior al espacio disponible del medio extraíble, el archivo abarcará varios dispositivos en función del espacio disponible en el medio. El archivo también se puede bloquear con una frase de contraseña. La recuperación a partir de un archivo no requiere un nuevo Core;cualquier Core puede ingerir el archivo y recuperar los datos si el administrador tiene la frase de contraseña y las claves de cifrado.

Virtualización y nube

Core es compatible con la tecnología en nube, que le permite aprovechar la capacidad informática de la nube para recuperación.

DL4000 puede exportar cualquier máquina protegida o replicada a una máquina virtual, como versiones con licencias de VMware o Hyper-V. Puede realizar una exportación virtual, o puede establecer una máquina en espera virtual VM mediante el establecimiento de una exportación virtual continua. Con exportaciones continuas, la máquina virtual se actualiza de modo incremental después de cada

instantánea. Las actualizaciones incrementales son muy rápidas y proporcionan clones en espera preparados para activarse con solo presionar un botón. Las exportaciones admitidas son tipos de máquina virtual VMware Workstation/Server en una carpeta, exportación directa a un host vSphere/ VMware ESX (i); exportación a Oracle VirtualBox; y exportación a Microsoft Hyper-V Server en Windows Server 2008 (x64), 2008 R2, 2012 (x64) y 2012 R2 (incluido el soporte para VM Hyper-V de segunda generación)

Además, ahora puede archivar los datos del repositorio en la nube mediante plataformas como Microsoft Azure, Amazon S3, Rackspace Cloud Block Storage u otros servicios en la nube basados en OpenStack.

Administración de alertas y eventos

Además de HTTP REST API, AppAssure también incluye un amplio conjunto de funciones para registro de eventos y notificación por correo electrónico, Syslog o Registro de eventos de Windows. Las notificaciones por correo electrónico pueden utilizarse para alertar a usuarios o grupos sobre la condición o estado de diferentes eventos en respuesta a una alerta. Los métodos Syslog y Registro de eventos de Windows se emplean para centralizar el registro en un repositorio en entornos con varios sistemas operativos; mientras que en entornos con Windows exclusivamente, solo se utiliza el Registro de eventos de Windows.

Portal de licencias

El Portal de licencias proporciona herramientas fáciles de usar para administrar los derechos de licencia. Puede descargar, activar, ver y administrar claves de licencia y crear un perfil de compañía para realizar un seguimiento de sus activos de licencia. Además, el portal permite a los proveedores de servicio y redistribuidores realizar un seguimiento y administrar sus licencias de cliente.

Consola web

DL4000 presenta una consola central basada en la web que administra Cores distribuidos desde una ubicación central. Los MSP y los clientes empresariales con varios Cores distribuidos pueden implementar la consola central para obtener una visión unificada de la administración central. La Central Management Console (Consola de administración central) permite la capacidad de organizar los Cores administrados en unidades organizativas jerárquicas. Estas unidades jerárquicas pueden representar unidades de negocio, ubicaciones o clientes para MSP con acceso basado en la función. La consola central también puede ejecutar informes entre Cores administrados.

API de administración de servicios

DL 4000 incluye una APIde administración de servicio y proporciona acceso programático a todas las funciones disponibles a través de la Central Management Console (Consola de administración central). La APIde administración de servicio es una APIde REST. Todas las operaciones de APIse realizan sobre SSL y se autentican mutuamente mediante certificados X.509 v3. Se puede acceeder al servicio de administración desde dentro del entorno o directamente a través de Internet desde cualquier aplicación que pueda enviar y recibir una solicitud y respuesta HTTPS. El enfoque facilita la fácil integración con aplicaciones web como herramientas de metodología de administración de relaciones (RMM) o sistemas de facturación. También se incluye un cliente de SDK para secuencias de comandos PowerShell.

2

Trabajar con DL4000 Core

Acceso a la DL4000 Core Console

Para acceder a Core Console:

1. Actualizar los sitios de confianza en el explorador. Consulte Actualización de los sitios de confianza en Internet Explorer.
2. Configure los exploradores para acceder de forma remota a Core Console. Consulte Configuración de exploradores para acceder de manera remota a Core Console.
3. Realice una de las siguientes acciones para acceder a Core Console:
   - Inicie sesión localmente en el servidor DL4000 Core y, a continuación, haga doble clic en el icono de **Core Console**.
   - Escriba una de las URL siguientes en el explorador de web:
     - **https://<NombredesuServidorCore>:8006/apprecovery/admin/core**
     - **https://<DirecciónIPdesuServidorCore>:8006/apprecovery/admin/core**

Actualización de los sitios de confianza en Internet Explorer

Para actualizar los sitios de confianza en Microsoft Internet Explorer:

1. Abra Internet Explorer.
2. Si **File (Archivo)**, **Edit View (Editar vista)** y demás menús no aparecen, presione <F10>.
3. Haga clic en el menú **Tools (Herramientas)** y seleccione **Internet Options (Opciones de Internet)**.
4. En la ventana **Internet Options (Opciones de Internet)**, haga clic en la pestaña **Security (Seguridad)**.
5. Haga clic en **Trusted Sites (Sitios de confianza)** y, a continuación, haga clic en **Sites (Sitios)**.
6. En **Add this website to the zone (Agregar este sitio web a la zona)**, introduzca **https://[Display Name]**, usando el nuevo nombre que haya proporcionado para el nombre de visualización.
7. Haga clic en **Add (Agregar)**.
8. En **Add this website to the zone (Agregar este sitio web a la zona)**, escriba **about:blank**.
9. Haga clic en **Add (Agregar)**.
10. Haga clic en **Close (Cerrar)** y, a continuación, en **OK (Aceptar)**.

Configuración de exploradores para acceder de manera remota a Core Console

Para acceder a la Core Console desde una máquina remota, primero debe modificar la configuración del explorador.

NOTA: Para modificar la configuración del explorador, inicie sesión en el sistema como administrador.

NOTA: Google Chrome utiliza la configuración de Microsoft Internet Explorer: deberá utilizar Internet Explorer para cambiar los valores de configuración del explorador Chrome.

NOTA: Cuando acceda a la consola web de Core, de manera local o remota, asegúrese de que esté activada **Internet Explorer Enhanced Security Configuration (Configuración de seguridad mejorada de Internet Explorer)**. Para activar la **Internet Explorer nhanced Security Configuration (Configuración de seguridad mejorada de Internet Explorer)**:

1. Abrir el **Server Manager (Administrador de servidores)**
2. Seleccione **Local Server IE Enhanced Security Configuration (Configuración de seguridad mejorada de Internet Explorer en servidor local)**, que se muestra a la derecha. Compruebe que está en **On (Activada)**.

Para modificar la configuración del explorador en Internet Explorer y en Chrome:

1. Abra Internet Explorer.
2. En el menú **Tools (Herramientas)**, seleccione las fichas **Internet Options (Opciones de Internet), Security (Seguridad)**.
3. Haga clic en **Trusted Sites (Sitios de confianza)** y, a continuación, haga clic en **Sites (Sitios)**.
4. Deseleccione la opción **Require server verification (https) for all sites in the zone (Requerir comprobación del servidor (https) para todos los sitios de esta zona)** y, a continuación, añada http://*<nombre del host o dirección IP del servidor que aloja AppAssure 5 Core>* a **Trusted Sites (Sitios de confianza)**.
5. Haga clic en **Close (Cerrar)**, seleccione **Trusted Sites (Sitios de confianza)** y, después, haga clic en **Custom Level (Nivel personalizado)**.
6. Desplácese hasta **Miscellaneous (Miscelánea)** → **Display Mixed Content (Mostrar contenido mixto)** y seleccione **Enable (Habilitar)**.
7. Desplácese a la parte inferior de la pantalla hasta **User Authentication (Autenticación del usuario)** → **Logon (Inicio de sesión)** y, a continuación, seleccione **Automatic logon with current user name and password (Inicio de sesión automático con el nombre de usuario y contraseña actuales)**.
8. Haga clic en **OK (Aceptar)** y, después, seleccione la pestaña **Advanced (Opciones avanzadas)**.
9. Vaya hasta **Multimedia** y seleccione **Play animations in webpages (Reproducir animaciones en páginas web)**.
10. Desplácese hasta **Security (Seguridad)**, active la opción **Enable Integrated Windows Authentication (Habilitar autenticación integrada de Windows)** y, a continuación, haga clic en **OK (Aceptar)**.

Para modificar la configuración del explorador Mozilla Firefox:

1. En la barra de direcciones de Firefox, escriba **about:config** y, a continuación, haga clic en **I'll be careful, I promise (¡Tendré cuidado, lo prometo!)** si aparece el cuadro de diálogo.
2. Busque el término **ntlm**.

   La búsqueda debería devolver al menos tres resultados.
3. Haga doble clic en **network.automatic-ntlm-auth.trusted-uris** y escriba la siguiente configuración según convenga para su máquina:
   - En las máquinas locales, introduzca el nombre de host.
   - En las máquinas remotas, escriba el nombre del host o la dirección IP, separados por comas, del servidor que aloja el AppAssure Core; por ejemplo, *dirección IP,nombre del host*.
4. Reinicie Firefox.

Planificación de la configuración del Core

La configuración incluye tareas como la creación y configuración del repositorio para almacenar instantáneas de copia de seguridad, definir claves de cifrado para asegurar los datos protegidos y

configurar alertas y notificaciones. Después de completar la configuración del Core, puede proteger los Agents y realizar la recuperación.

La configuración del Core implica comprender varios conceptos y realizar las operaciones iniciales siguientes:

- Crear un repositorio
- Configurar claves de cifrado
- Configurar notificación de eventos
- Configurar la política de retención
- Configurar la conectabilidad de SQL

NOTA: Si está utilizando el servidor DL4000, se recomienda utilizar la pestaña **Appliance** para configurar el Core. Para obtener más información acerca de la configuración del Core, después de la instalación inicial, consulte la *Dell DL4000 Appliance Deployment Guide* (Guía de implementación del appliance Dell DL4000) en **dell.com/support/home**.

Administración de licencias

Puede administrar sus licencias directamente desde la Core Console. Desde la consola, puede cambiar la clave de licencia y ponerse en contacto con el servidor de licencias. También puede acceder al Portal de licencias desde la página Licensing (Licencias) de la consola Core.

La página Licensing (Licencias) incluye la información siguiente:

- License type (Tipo de licencia)
- License status (Estado de licencia)
- Restricciones de la licencia
- Number of machines protected (Número de máquinas protegidas)
- Status of last response from the licensing server (Estado de la última respuesta desde el servidor de licencias)
- Time of last contact with the licensing server (Hora del último contacto con el servidor de licencias)
- Next scheduled attempt of contact with the licensing server (Siguiente intento programado para el contacto con el servidor de licencias)

Cambio de una clave de licencia

Para cambiar una clave de licencia:

1. Vaya a la Core Console.
2. Seleccione **Configuration (Configuración)** → **Licensing (Licencias)**.

   Aparecerá la página **Licensing (Licencias)**.
3. En la sección **License Details (Detalles de la licencia)**, haga clic en **Change License (Cambiar licencia)**.

   Aparecerá el cuadro de diálogo **Change License (Cambiar licencia)**.
4. En el cuadro de diálogo **Change License (Cambiar licencia)**, introduzca la nueva clave de licencia y haga clic en **OK (Aceptar)**.

Cómo ponerse en contacto con el servidor del portal de licencias

Core Console se pone en contacto con el servidor del portal frecuentemente para mantenerse al día sobre cualquier cambio que se realice en el portal de licencias. Normalmente, la comunicación con el

servidor del portal se produce automáticamente en los intervalos designados; no obstante, puede iniciar la comunicación bajo demanda.

Para establecer contacto con el servidor del portal:

1. Vaya a la Core Console.
2. Haga clic en **Configuration (Configuración)** → **Licensing (Licencias)**.
3. En la opción **License Server (Servidor de licencias)**, haga clic en **Contact Now (Establecer contacto ahora)**.

Administración de la configuración del Core

La configuración del Core se utiliza para definir diversos valores para la configuración y el rendimiento. La mayoría de los valores se configuran para uso óptimo, pero pueden cambiar los siguientes valores según sea necesario:

- General
- Nightly Jobs (Trabajos nocturnos)
- Transfer Queue (Cola de transferencias)
- Client Timeout Settings (Configuración del tiempo de espera del cliente)
- Deduplication Cache Configuration (Configuración de la caché de desduplicación)
- Database Connection Settings (Configuración de conexión de base de datos)

Cómo cambiar el nombre de visualización del Core

NOTA: Es recomendable seleccionar un nombre de visualización permanente durante la configuración inicial del servidor DL4000. Si lo cambia posteriormente, deberá realizar algunos pasos manualmente para asegurarse de que el nuevo nombre de host surta efecto y el servidor funcione correctamente. Para obtener más información, consulte Cómo cambiar el nombre de host manualmente).

Para cambiar el nombre de visualización del Core:

1. Vaya a Core Console.
2. Haga clic en **Configuration (Configuración)** → **Settings (Valores)**
3. En el panel **General (General)**, haga clic en **Change (Cambiar)**.

   Aparecerá el cuadro de diálogo **General Settings (Configuración general)**.
4. En el cuadro de texto **Display Name (Nombre de visualización)**, introduzca el nuevo nombre de visualización para el Core.

   Este es el nombre que se mostrará en la Core Console. Puede introducir hasta 64 caracteres.
5. En el campo **Web Server Port (Puerto de servidor web)** , introduzca un número de puerto para el servidor Web. El valor predeterminado es 8006.
6. En el **Service Port (Puerto de servicio)**, introduzca un número de puerto para el servicio. El valor predeterminado es 8006.
7. Haga clic en **OK (Aceptar)**.

Ajuste de la hora de los trabajos nocturnos

Para ajustar la hora de los trabajos nocturnos:

1. Vaya a Core Console.
2. Haga clic en **Configuration (Configuración)** → **Settings (Valores)**.

3. En el área **Nightly Jobs (Trabajos nocturnos)**, haga clic en **Change (Cambiar)**.

   Aparecerá el cuadro de diálogo **Nightly Jobs (Trabajos nocturnos)**.
4. En el cuadro de texto **Nightly Jobs Time (Hora de los trabajos nocturnos)**, especifique la nueva hora para realizar los trabajos nocturnos.
5. Haga clic en **OK (Aceptar)**.

Modificación de la configuración de la cola de transferencias

La configuración de la cola de transferencias representa los ajustes básicos que definen el número máximo de transferencias simultáneas y el número máximo de reintentos para los datos que se van a transferir.

Para modificar la configuración de la cola de transferencias:

1. Vaya a Core Console.
2. Haga clic en **Configuration (Configuración)** → **Settings (Valores)**.
3. En el área **Transfer Queue (Cola de transferencias)**, haga clic en **Change (Cambiar)**.

   Aparecerá el cuadro de diálogo **Transfer Queue (Cola de transferencias)**.
4. En el cuadro de texto **Maximum Concurrent Transfers (Número máximo de transferencias simultáneas)**, introduzca un valor para actualizar el número de transferencias simultáneas.

   Escriba un número entre 1 y 60. Cuanto más pequeño sea el número, menor será la carga en la red y en otros recursos del sistema. A medida que aumente la capacidad que se procesa, también aumentará la carga en el sistema.
5. En el cuadro de texto **Maximum Retries (Número máximo de reintentos)**, introduzca un valor para actualizar el número máximo de reintento.
6. Haga clic en **OK (Aceptar)**.

Ajuste de la configuración del tiempo de espera del cliente

Para ajustar la configuración del tiempo de espera del cliente:

1. Vaya a Core Console.
2. Haga clic en **Configuration (Configuración)** → **Settings (Valores)**.
3. En el área **Client Timeout Settings Configuration (Configuración de los valores del tiempo de espera del cliente)**, haga clic en **Change (Cambiar)**.

   Se abrirá el cuadro de diálogo **Client Timeout Settings (Configuración del tiempo de espera del cliente)**.
4. En el cuadro de texto **Connection Timeout (Tiempo de espera de la conexión)**, introduzca el número de minutos y segundos que transcurrirán antes de que se agote el tiempo de espera de la conexión.
5. En el cuadro de texto **Connection UI Timeout (Tiempo de espera de la interfaz de usuario de la conexión)**, introduzca el número de minutos y segundos que transcurrirán antes de que se agote el tiempo de espera de la interfaz de usuario de la conexión.
6. En el cuadro de texto **Read/Write Timeout (Tiempo de espera de lectura/escritura)**, introduzca el número de minutos y segundos que desea que transcurran antes de que se agote el tiempo de espera durante un evento de lectura/escritura.
7. En el cuadro de texto **Read/Write UI Timeout (Tiempo de espera de la interfaz de usuario de lectura/escritura**), especifique el número de minutos y segundos que transcurrirán antes de que se agote el tiempo de espera de la interfaz de usuario de la lectura/escritura.
8. Haga clic en **OK (Aceptar)**.

Configuración de los valores de caché de la desduplicación

Para configurar los valores de caché de la desduplicación:

1. Vaya a Core Console.
2. Haga clic en **Configuration (Configuración)** → **Settings (Valores)**
3. En el área **Deduplication Cache Configuration (Configuración de la caché de desduplicación)**, haga clic en **Change (Cambiar)**.

   Aparecerá el cuadro de diálogo **Deduplication Cache Configuration (Configuración de la caché de desduplicación)**.
4. En el cuadro de texto **Primary Cache Location (Ubicación primaria de la caché)**, introduzca un valor actualizado para cambiar la ubicación primaria de la caché.
5. En el cuadro de texto **Secondary Cache Location (Ubicación secundaria de la caché)**, introduzca un valor actualizado para cambiar la ubicación secundaria de la caché.
6. En el cuadro de texto **Metadata Cache Location (Ubicación de metadatos de la caché)**, introduzca un valor actualizado para cambiar la ubicación de los metadatos de la caché.
7. En el cuadro de texto **Dedupe Cache Size (Tamaño de caché de desduplicación)**, introduzca un valor correspondiente a la cantidad de espacio que desea asignar para la caché de desduplicación.

   En el campo desplegable del tamaño de la unidad, seleccione GB (gigabytes) o TB (terabytes), indique la unidad de medida para el valor en el cuadro de texto Dedupe Cache Size (Tamaño de caché de desduplicación).
8. Haga clic en **OK (Aceptar)**.

   NOTA: Debe reiniciar el servicio del Core para que los cambios surjan efecto.

Modificación de la configuración del motor

Para modificar la configuración del motor:

1. Vaya a Core Console.
2. Haga clic en **Configuration (Configuración)** → **Settings (Valoración)**
3. En el área **Replay Engine Configuration (Configuración del motor de reproducción)**, haga clic en **Change (Cambiar)**.

   Aparecerá el cuadro de diálogo **Replay Engine Configuration (Configuración del motor de reproducción)**.
4. Introduzca la información de configuración, según se describe a continuación:

Cuadro de texto	Descripción
Dirección IP	• Para usar la dirección IP preferente de TCP/IP, haga clic en **Automatically Determined (Determinado automáticamente)**. • Para introducir manualmente una dirección IP, haga clic en **Use a specific address (Utilizar una dirección específica)**.
Preferable Port	Introduzca un número de puerto o acepte el valor predeterminado (el puerto predeterminado es 8007). El puerto se utiliza para especificar el canal de comunicación del motor.

Cuadro de texto	Descripción
Port in use (Puerto en uso)	Representa el puerto que está en uso para la configuración de motor de reproducción.
Allow port auto-assigning (Permitir la asignación automática de puerto)	Haga clic para permitir la asignación automática del puerto TCP.
Admin Group (Grupo de administración)	Introduzca un nombre nuevo para el grupo de administración. El nombre predeterminado es **BUILTIN\Administrators**.
Minimum Async I/O Length (Longitud de E/S asíncrona mínima)	Introduzca un valor o seleccione el valor predeterminado. Describe la longitud de entrada/salida asíncrona mínima. El valor predeterminado es 65536.
Receive Buffer Size (Tamaño de búfer de recepción)	Especifíque un tamaño de búfer de entrada o acepte el valor predeterminado. El valor predeterminado es 8192.
Send Buffer Size (Tamaño de búfer de envío)	Especifique un tamaño de búfer de salida o acepte el valor predeterminado. El valor predeterminado es 8192.
Read Timeout (Tiempo de espera de lectura)	Introduzca un valor de tiempo de espera de lectura o elija el valor predeterminado. Este es 00:00:30.
Write Timeout (Tiempo de espera de escritura)	Introduzca un valor de tiempo de espera de escritura o elija el valor predeterminado. Este es 00:00:30.
No Delay (Sin retraso)	Se le recomienda que deje esta casilla de verificación no seleccionada, ya que de otro modo tendrá un gran impacto en la eficiencia de la red. Si determina que necesita modificar este valor, póngase en contacto con Dell Support para obtener orientación.

5. Haga clic en **OK (Aceptar)**.

Modificación de la configuración de la conexión con la base de datos

Para modificar la configuración de la conexión con la base de datos:

1. Vaya a Core Console.
2. Haga clic en **Configuration (Configuración)** → **Settings (Valores)**
3. En el área **Database Connection Settings (Configuración de conexión de base de datos)**, realice una de las acciones siguientes:
   - Haga clic en **Apply Default (Aplicar valor predeterminado)**.
   - Haga clic en **Change (Cambiar)**.

Aparecerá el cuadro de diálogo **Database Connection Settings (Configuración de conexión de base de datos)**.

4. Introduzca la configuración para modificar la conexión con la base de datos como se describe a continuación:

Cuadro de texto	Descripción
Nombre del host	Introduzca un nombre de host para la conexión de la base de datos.
Port	Especifique un número de puerto para la conexión de la base de datos.
User Name (optional) (Nombre de usuario [opcional])	Introduzca un nombre de usuario para acceder y administrar la configuración de conexión de la base de datos. Se utiliza para especificar las credenciales de inicio de sesión para acceder a la conexión con la base de datos.
Password (optional) (Contraseña) [opcional])	Introduzca una contraseña para acceder y administrar la configuración de conexión de la base de datos.
Retain event and job history for, days (Retener evento e historial de trabajo durante, días)	Introduzca el número de días que se conservará el historial de eventos y trabajos de la conexión de la base de datos.
Max connection pool size (Tamaño máximo de grupo de conexiones)	Establece el número máximo de conexiones de bases de datos almacenadas en la memoria caché para permitir la reutilización dinámica. El valor predeterminado es 100.
Min connection pool size (Tamaño mínimo de grupo de conexiones)	Establece el número mínimo de conexiones de bases de datos almacenadas en la memoria caché para permitir la reutilización dinámica. El valor predeterminado es 0.

5. Haga clic en **Test Connection (Probar conexión)** para verificar la configuración.
6. Haga clic en **Save (Guardar)**.

Acerca de los repositorios

Un repositorio sirve para almacenar las instantáneas que se capturan desde sus estaciones de trabajo y servidores protegidos. El repositorio puede residir en diferentes tecnologías de almacenamiento, como por ejemplo Storage Area Network (Red de área de almacenamiento - SAN), Direct Attached Storage (Almacenamiento conectado directamente - DAS) o Network Attached Storage (Almacenamiento conectado a la red - NAS).

Cuando se crea el repositorio, el Core preasigna el espacio de almacenamiento necesario para los datos y metadatos en la ubicación especificada. Puede crear hasta 255 repositorios independientes en un Core individual utilizando diversas tecnologías de almacenamiento diferentes. Además, puede aumentar adicionalmente el tamaño de un repositorio al agregar nuevas extensiones o especificaciones de

archivos. Un repositorio ampliado puede contener hasta 4096 extensiones que abarcan diferentes tecnologías de almacenamiento.

Los conceptos y consideraciones clave del repositorio incluyen:

- El repositorio se basa en el AppAssure Scalable Object File System (Sistema de archivos de objeto ampliable de AppAssure).
- Todos los datos almacenados en un repositorio se desduplican globalmente.
- El Scalable Object File System (Sistema de archivos de objeto ampliable) puede ofrecer rendimiento ampliable de E/S junto con desduplicación global de datos, Core y administración de retención.

NOTA: Los repositorios de DL4000 se almacenan en dispositivos de almacenamiento primarios. No se admiten dispositivos de almacenamiento de archivado como Data Domain (Dominio de datos), debido a limitaciones de rendimiento. De forma similar, no deben almacenarse repositorios en archivadores NAS que se vinculen con la nube, puesto que estos dispositivos suelen presentar limitaciones de rendimiento cuando se utilizan como almacenamiento primario.

Plan para administrar un repositorio

Las directrices para administrar un repositorio cubren tareas como crear, configurar y ver un repositorio, e incluyen los temas siguientes:

- Acceso a Core Console
- Creación de un repositorio
- Visualización de los detalles de un repositorio
- Modificación de la configuración del repositorio
- Cómo agregar una ubicación de almacenamiento a un repositorio existente
- Comprobación de un repositorio
- Eliminación de un repositorio
- Recuperación de un repositorio

NOTA: Se recomienda que utilice la pestaña **Appliance** para configurar los repositorios.

Antes de comenzar a usar el appliance DL4000, debe configurar uno o más repositorios en el servidor Core. Un repositorio almacena sus datos protegidos. En concreto, almacena las instantáneas capturadas desde los servidores protegidos en su entorno.

Cuando configure un repositorio, podrá realizar varias tareas, como por ejemplo: especificar dónde se ubicará el almacenamiento de datos en el servidor del Core, cuántas ubicaciones pueden agregarse a cada repositorio, el nombre del repositorio, cuántas operaciones actuales admitirán los repositorios, etc.

Cuando se crea un repositorio, el Core preasigna el espacio necesario para almacenar datos y metadatos en la ubicación especificada. Puede crear hasta 255 repositorios independientes en un Core individual. Puede agregar nuevas ubicaciones o volúmenes de almacenamiento para ampliar adicionalmente el tamaño de un repositorio individual.

Puede agregar o modificar repositorios en Core Console.

Creación de un repositorio

NOTA: Si está utilizando el servidor DL4000 como un SAN, se recomienda utilizar la pestaña **Appliance** para configurar los repositorios. Para ello, puede utilizar el siguiente procedimiento para configurar manualmente el almacenamiento.

Para crear un repositorio:

1. Vaya a Core Console.
2. Haga clic en **Configuration (Configuración)** → **Repositories (Repositorios)**.
3. Haga clic en **Add new (Agregar nuevo)**.
   Aparecerá el cuadro de diálogo **Add New Repository (Agregar repositorio nuevo)**.
4. Introduzca la información según se describe en la tabla siguiente.

Cuadro de texto	Descripción
Repository Name (Nombre del repositorio)	Introduzca el nombre de visualización del repositorio. De manera predeterminada, este cuadro de texto se compone de la palabra Repository y un número de índice, que agrega un número de manera secuencial al repositorio nuevo, empezando en 1. Puede cambiar el nombre según sea necesario. Puede introducir hasta 150 caracteres.
Concurrent Operations (Operaciones concurrentes)	Define el nombre de solicitudes concurrentes que desea que admita el repositorio. De manera predeterminada, el valor es 64.
Comments (Comentarios)	Opcionalmente, introduzca una nota descriptiva sobre este repositorio.

5. Para establecer el volumen o ubicación de almacenamiento específica para el repositorio, haga clic en **Add Storage Location (Agregar ubicación de almacenamiento)**.

   PRECAUCIÓN: Si el repositorio de AppAssure que va a crear en este paso se elimina más tarde, se eliminarán todos los archivos de la ubicación de almacenamiento del repositorio. Si no establece ninguna carpeta específica para almacenar los archivos del repositorio, éstos se almacenarán en la raíz. Si se elimina el repositorio, también se eliminará todo el contenido de la raíz, lo que provocará una pérdida muy grave de datos.

   NOTA: Los repositorios se almacenan en dispositivos de almacenamiento primarios. No se admiten dispositivos de almacenamiento de archivado como Data Domain (Dominio de datos), debido a limitaciones de rendimiento. De forma similar, no deben almacenarse repositorios en archivadores NAS que se vinculen con la nube, puesto que estos dispositivos suelen presentar limitaciones de rendimiento cuando se utilizan como almacenamiento primario.

   Se muestra el cuadro de diálogo **Add Storage Location (Agregar ubicación de almacenamiento)**.
6. Especifique cómo se agregará el archivo para la ubicación de almacenamiento. Puede elegir agregar el archivo en el disco local o en recurso compartido CIFS.
   - Para especificar una máquina local, haga clic en **Add file on local disk (Agregar archivo en disco local)** y, después, introduzca la información según se indica a continuación:

Cuadro de texto	Descripción
Data Path (Ruta de acceso datos)	Introduzca la ubicación para almacenar los metadatos protegidos; por ejemplo, escriba **X:\Repository\Data**. Al especificar la ruta, escriba solo caracteres alfanuméricos, un guión o un punto (para separar los nombres de host de los dominios). Las letras de la "a" a la "z" no distinguen mayúsculas de minúsculas. No utilice espacios. No se admite ningún otro símbolo o caracteres de puntuación.
Metadata Path (Ruta de acceso a metadatos)	Introduzca la ubicación para almacenar los metadatos protegidos; por ejemplo, escriba **X:\Repository\Metadata**. Al especificar la ruta, escriba solo caracteres alfanuméricos, un guión o un punto (para separar los nombres de host de los dominios). Las letras de la "a" a la "z" no distinguen mayúsculas de minúsculas. No utilice espacios. No se admite ningún otro símbolo o caracteres de puntuación.

- O bien, para indicar una ubicación en un recurso compartido, haga clic en **Add file on CIFS share (Agregar archivo en recurso compartido CIFS)** y, después, introduzca la información según se indica a continuación:

Cuadro de texto	Descripción
UNC Path (Ruta de acceso a UNC)	Introduzca la ruta de acceso para la ubicación del recurso compartido de red. Si la ubicación se encuentra en la raíz, cree un nombre de carpeta dedicado (por ejemplo, Repositorio). La ruta de acceso debe comenzar por \\. Al especificar la ruta, escriba solo caracteres alfanuméricos, un guión o un punto (para separar los nombres de host de los dominios). Las letras de la "a" a la "z" no distinguen mayúsculas de minúsculas. No utilice espacios. No se admite ningún otro símbolo o caracteres de puntuación.
User Name (Nombre de usuario)	Especifique un nombre de usuario para el acceso a la ubicación del recurso compartido de red.
Contraseña	Especifique una contraseña para acceder a la ubicación del recurso compartido de red.

7. En el panel **Details (Detalles)**, haga clic en **Show/Hide Details (Mostrar u ocultar detalles)** e introduzca los detalles para la ubicación de almacenamiento, según se describe a continuación:

Cuadro de texto	Descripción
Tamaño	Establezca el tamaño o capacidad para la ubicación de almacenamiento. El tamaño predeterminado es 250 MB. Puede elegir entre: • MB • GB • TB **NOTA:** El tamaño que especifique no puede superar el tamaño del volumen.

Cuadro de texto	Descripción
	NOTA: Si la ubicación de almacenamiento es un volumen de sistema de archivos de nueva tecnología (NTFS) que tiene Windows XP o Windows 7 instalado, el límite de tamaño de archivo es 16 TB. Si la ubicación de almacenamiento es un volumen NTFS que tiene Windows 8 o Windows Server 2012 instalado, el límite de tamaño de archivo es 256 TB. NOTA: Para validar el sistema operativo, el Instrumental de administración de Windows (WMI) debe estar instalado en la ubicación de almacenamiento deseada.
Write Caching Policy (Política de escritura en caché)	La política de escritura en caché de controla cómo se utiliza el Windows Cache Manager (Administrador de caché de Windows) en el repositorio y ayuda a ajustar el repositorio para un rendimiento óptimo en diferentes configuraciones. Establezca el valor en una de las opciones siguientes: • On (Activado) • Off (Desactivado) • Sync (Sincronizar) Si el valor se establece en On (Activado), que es el valor predeterminado, Windows controla el almacenamiento en caché. NOTA: Si se establece la política de escritura en caché en On (Activado), se mejora el rendimiento. Si usa una versión de Windows Server anterior a Server 2012, la configuración recomendada es **Off (Desactivado)**. Si se establece en **Off (Desactivado)**, AppAssure controla el almacenamiento en caché. Si se establece en **Sync (Sincronizar)**, Windows controla el almacenamiento en caché así como la entrada/salida sincrónica.
Bytes por sector (Bytes por sector)	Especifique el número de bytes que desee incluir en cada sector. El valor predeterminado es 512.
Average Bytes per Record (Promedio de bytes por registro)	Especifique el número promedio de bytes por segundo. El valor predeterminado es 8192.

8. Haga clic en **Save (Guardar)**.
   Se muestra la pantalla **Repositories (Repositorios)** e incluirá la ubicación de almacenamiento recién agregada.
9. Repita del paso 4 al paso 7 para agregar más ubicaciones de almacenamiento para el repositorio.
10. Haga clic en **Create (Crear)** para crear el repositorio.
    La información de **Repository (Repositorio)** aparecerá en la pestaña **Configuration (Configuración)**.

Visualización de los detalles de un repositorio

Para ver los datos de un repositorio:

1. Vaya a la Core Console.
2. Haga clic en **Configuration (Configuración)** → **Repositories (Repositorios)**.
3. Haga clic en el símbolo **>** situado junto a la columna **Status (Estado)** del repositorio para el que desea ver los detalles.
4. En la vista ampliada, puede realizar las siguientes acciones:
   - Modificar la configuración
   - Añadir una ubicación de almacenamiento
   - Comprobar un repositorio
   - Eliminar un repositorio

   También se muestran otros datos del repositorio, como la ubicación de almacenamiento y las estadísticas. Entre los datos de la ubicación de almacenamiento se incluye la ruta de acceso a metadatos, la ruta de acceso a datos y el tamaño. Entre la información estadística se incluye:
   - Desduplicación: número de aciertos de desduplicación de bloques y de desaciertos de desduplicación de bloques y la velocidad de compresión de bloques.
   - E/S de registro: que incluye la velocidad (MB/s), la velocidad de lectura (MB/s) y la velocidad de escritura (MB/s).
   - Motor de almacenamiento: que notifica la velocidad (MB/s), la velocidad de lectura (MB/s) y la velocidad de escritura (MB/s).

Modificación de la configuración del repositorio

Después de agregar un repositorio, puede modificar la configuración del repositorio, como por ejemplo la descripción o el número máximo de operaciones concurrentes. También puede crear una ubicación de almacenamiento nueva para el repositorio.

Para modificar la configuración del repositorio:

1. Vaya a Core Console.
2. Haga clic en **Configuration (Configuración)** → **Repositories (Repositorios)**.
3. Haga clic en el icono Settings (Configuración) junto a la columna Compression Ratio (Relación de compresión) debajo del botón **Actions (Acciones)** y, a continuación, en **Settings (Valores)**.

   Aparecéra el cuadro de diálogo **Repository Settings (Configuración del repositorio)**.
4. Introduzca la información del repositorio, según se describe a continuación:

Campo	Descripción
Repository Name (Nombre del repositorio)	Representa el nombre de visualización del repositorio. De manera predeterminada, este cuadro de texto se compone de la palabra Repository y un número de índice, que se corresponde con el número del nuevo repositorio. NOTA: No puede editar el nombre del repositorio.
Descripción	Opcionalmente, introduzca una nota descriptiva sobre el repositorio.

Campo	Descripción
Maximum Concurrent Operations (Número máximo de operaciones concurrentes)	Defina el número de solicitudes concurrentes que desee que admita el repositorio.
Enable Deduplication (Habilitar la desduplicación)	Para desactivar la desduplicación, desmarque esta casilla. Si desea habilitar la desduplicación, márquela. NOTA: Si cambia este valor solo se aplicará a las copias de seguridad que se realicen después de realizar el cambio. Los datos existentes, o los datos replicados desde otro Core o importados desde un archivo, mantienen los valores de desduplicación vigentes en el momento en el que se capturaron los datos desde el Agent.
Enable Compression (Habilitar la compresión)	Para desactivar la compresión, desmarque esta casilla. Si desea habilitar la compresión, márquela. NOTA: Este valor solo se aplicará a las copias de seguridad que se realicen después de cambiar el valor. Los datos existentes, o los datos replicados desde otro Core o importados desde un archivo, mantienen los valores de compresión vigentes en el momento en el que se capturaron los datos desde el Agent.

5. Haga clic en **Save (Guardar)**.

Ampliación de un repositorio existente

Si añade otro DAS MD1200 al servidor DL4000, puede utilizar el almacenamiento disponible para ampliar el repositorio existente.

Para ampliar un repositorio existente:

1. Después de instalar el DAS MD1200, abra la Core Console, seleccione la pestaña **Appliance** y, a continuación, haga clic en **Tasks (Tareas)**.
2. En la pantalla **Tasks (Tareas)**, junto al nuevo almacenamiento, haga clic en **Provision (Aprovisionamiento)**.
3. En la pantalla **Provisioning Storage (Aprovisionamiento de almacenamiento)**, seleccione **Expand the existing repository (Ampliar el repositorio existente)** y, a continuación, elija el repositorio que desea ampliar.
4. Haga clic en **Provision (Aprovisionar)**.

   En la pantalla **Tasks (Tareas)** se mostrará la **Status Description (Descripción de estado)** al lado del dispositivo de almacenamiento como **Provisioned (Aprovisionado)**.

Cómo agregar una ubicación de almacenamiento a un repositorio existente

Al agregar una ubicación de almacenamiento, es posible definir dónde desea almacenar el repositorio o volumen.

Para agregar una ubicación de almacenamiento a un repositorio existente:

1. Haga clic en el símbolo **>** situado junto a la columna **Status (Estado)** del repositorio para el que desea agregar una ubicación de almacenamiento.
2. Haga clic en **Add Storage Location (Agregar ubicación de almacenamiento)**.

   Aparecerá el cuadro de diálogo **Add Storage Location (Agregar ubicación de almacenamiento)**.
3. Especifique cómo se agregará el archivo para la ubicación de almacenamiento. Puede elegir agregar el archivo en el disco local o en un recurso compartido CIFS.
   - Para indicar una máquina local, haga clic en **Add file on local disk (Agregar archivo en disco local)** y, después, introduzca la información según se indica a continuación:

Cuadro de texto	Descripción
Metadata Path (Ruta de acceso a metadatos)	Introduzca la ubicación para almacenar los metadatos protegidos.
Data Path (Ruta de acceso datos)	Introduzca la ubicación para almacenar los datos protegidos.

   - Para indicar una ubicación en un recurso compartido, haga clic en **Add file on CIFS share (Agregar archivo en recurso compartido CIFS)** y, después, introduzca la información según se indica a continuación:

Cuadro de texto	Descripción
UNC Path (Ruta de acceso a UNC)	Introduzca la ruta de acceso para la ubicación del recurso compartido de red.
User Name (Nombre de usuario)	Especifique un nombre de usuario para el acceso a la ubicación del recurso compartido de red.
Contraseña	Especifique una contraseña para acceder a la ubicación del recurso compartido de red.

4. En la sección **Details (Detalles)**, haga clic en **Show/Hide Details (Mostrar u ocultar detalles)** e introduzca los detalles para la ubicación de almacenamiento, según se describe a continuación:

Cuadro de texto	Descripción
Tamaño	Establezca el tamaño o capacidad para la ubicación de almacenamiento. El tamaño predeterminado es 250 MB. Puede elegir entre: • MB • GB • TB NOTA: El tamaño que especifique no puede superar el tamaño del volumen. NOTA: Si la ubicación de almacenamiento es un volumen NTFS que tiene Windows XP o Windows 7 instalado, el límite de tamaño de archivo es 16 TB. Si la ubicación de almacenamiento es un volumen NTFS que tiene Windows 8 o Windows Server 2012 instalado, el límite de tamaño de archivo es 256 TB.

Cuadro de texto	Descripción
	NOTA: Para validar el sistema operativo, WMI debe estar instalado en la ubicación de almacenamiento deseada.
Write Caching Policy (Política de escritura en caché)	La política de escritura en caché controla cómo se utiliza el Windows Cache Manager (Administrador de caché de Windows) en el repositorio y ayuda a ajustar el repositorio para un rendimiento óptimo en diferentes configuraciones. Establezca el valor en una de las opciones siguientes: • On (Activado) • Off (Desactivado) • Sync (Sincronizar) Si se establece en **On (Activado)**, que es el valor predeterminado, Windows controla el almacenamiento en caché. NOTA: Si se establece la política de escritura en caché en **On (Activado)**, se mejora el rendimiento; no obstante, el valor recomendado es **Off (Desactivado)**. Si se establece en **Off (Desactivado)**, AppAssure controla el almacenamiento en caché. Si se establece en **Sync (Sincronizar)**, Windows controla el almacenamiento en caché así como la entrada/salida sincrónica.
Bytes por sector (Bytes por sector)	Especifique el número de bytes que desee incluir en cada sector. El valor predeterminado es 512.
Average Bytes per Record (Promedio de bytes por registro)	Especifique el número promedio de bytes por segundo. El valor predeterminado es 8192.

5. Haga clic en **Save (Guardar)**.
   Se muestra la pantalla **Repositories (Repositorios)** e incluirá la ubicación de almacenamiento recién agregada.
6. Repita del paso 4 al paso 7 para agregar más ubicaciones de almacenamiento para el repositorio.
7. Haga clic en **OK (Aceptar)**.

Comprobación de un repositorio

DL4000 puede realizar una comprobación de diagnóstico de un volumen de repositorio cuando se producen errores. Los errores del Core pueden ser el resultado de un apagado incorrecto o un error de hardware, entre otros motivos.

NOTA: Este procedimiento se debe realizar únicamente con fines de diagnóstico.

Para comprobar un repositorio:

1. En la pesetaña **Configuration (Configuración)**, haga clic en **Repositories (Repositorios)**y, a continuación, seleccione **>** junto al repositorio que desea comprobar.
2. En el panel **Actions (Acciones)**, haga clic en **Check (Comprobar)**.
   Aparecerá el cuadro de diálogo **Check Repository (Comprobar repositorio)**.

3. En el cuadro de diálogo **Check Repository (Comprobar repositorio)**, haga clic en **Check (Comprobar)**.

   NOTA: Si la comprobación falla, restaure el repositorio desde un archivo.

Eliminación de un repositorio

Para eliminar un repositorio:

1. En la pestaña **Configuration (Configuración)**, haga clic en **Repositories (Repositorios)**y, a continuación, seleccione **>** junto al repositorio que desea eliminar.
2. En el panel **Actions (Acciones)**, haga clic en **Delete (Eliminar)**.
3. En el cuadro de diálogo **Delete Repository (Eliminar repositorio)**, haga clic en **Delete (Eliminar)**.

   PRECAUCIÓN: Cuando se elimina un repositorio, los datos del mismo se descartan y no se pueden recuperar.

   Cuando se elimina un repositorio, entonces debe ir a través de Open Manage System Administrator y eliminar los discos virtuales que alojan el repositorio. Después de eliminar los discos virtuales, puede volver a aprovisionar los discos y, a continuación, vuelva a crear el repositorio.

Cómo volver a montar volúmenes

Para volver a montar volúmenes:

1. Vaya a la Core Console.
2. **Appliance → Tasks (Tareas del servidor)**.
3. Haga clic en **Remount Volumes (Volver a montar volúmenes)**.

   Los volúmenes se vuelven a montar.

Cómo resolver volúmenes externos

Si un equipo MD1200 aprovisionado se apaga o desconecta y se vuelve a encender después, se muestra un evento en la Core Console que indica que el MD1200 está conectado. Sin embargo, no aparece ninguna tarea en la pestaña **Appliance** de la pantalla **Tasks (Tareas)** que le permita recuperarlo. La pantalla **Enclosures (Gabinetes)** muestra que el MD1200 se encuentra en estado "externo" y los repositorios de los discos virtuales externos están sin conexión.

Para resolver los volúmenes externos:

1. En la Core Console, seleccione la pestaña **Appliance** y, a continuación, haga clic en **Remount Volumes (Volver a montar volúmenes)**.

   Los volúmenes se vuelven a montar.
2. Seleccione la pestaña **Configuration (Configuración)** y, a continuación, haga clic en **Repositories (Repositorios)**.
3. Expanda el repositorio con el indicador de estado rojo. Para ello, haga clic en el símbolo **>** al lado de **Status (Estado)**.
4. Para verificar la integridad del repositorio, en **Actions (Acciones)**, haga clic en **Check (Comprobar)**.

Recuperación de un repositorio

Cuando DL4000 genera un error al importar un repositorio, informa acerca del error en la pantalla **Tasks (Tareas)** e indica el estado con un círculo rojo y con el mensaje **Error, Completed — Exception (Error, completado: excepción)**. Para ver los detalles del error en la pantalla **Tasks (Tareas)**, amplíe los datos de

la tarea haciendo clic en el símbolo **>** que aparece junto a la columna **Status (Estado)**. La sección **Status Details (Detalles de estado)** muestra que el estado de la tarea de recuperación es una excepción, y en la columna **Error Message (Mensaje de error)** se proporcionan más detalles sobre la condición de error.

Para recuperar un repositorio de un estado de importación erróneo:

1. Vaya a la Core Console.

   En la ventana **Repositories (Repositorios)** aparece el repositorio erróneo con un indicador de estado en rojo.
2. Haga clic en **Configuration (Configuración)** → **Repositories (Repositorios)**.
3. Para ampliar el repositorio erróneo, haga clic en el símbolo **>** junto a **Status (Estado)**.
4. En la sección **Actions (Acciones)**, haga clic en **Check (Comprobar)** y, a continuación, haga clic en **Yes (Sí)** para confirmar que desea realizar la comprobación.

   DL4000 recupera el repositorio.

Administración de la seguridad

Core puede cifrar datos de instantáneas del Agent en el repositorio. En lugar de cifrar todo el repositorio, puede especificar una clave de cifrado durante la protección de un Agent en un repositorio, lo que le permite volver a utilizar las claves para diferentes Agents. El cifrado no afecta al rendimiento, porque cada clave de cifrado activa crea un dominio de cifrado. Esto permite que un Core individual admita varios clientes al alojar varios dominios de cifrado. En un entorno con múltiples clientes, los datos se particionan y desduplican dentro de los dominios de cifrado. Puesto que usted administra las claves de cifrado, la pérdida del volumen no puede revelar las claves. Entre los conceptos y consideraciones sobre la seguridad de las claves se incluyen:

- El cifrado se realiza mediante AES de 256 bits en el modo Encadenamiento de bloques de cifrado (CBC) que cumple SHA-3.
- La desduplicación funciona en el dominio de Core para garantizar la privacidad.
- El cifrado se realiza sin afectar al rendimiento.
- Puede agregar, quitar, importar, exportar, modificar y eliminar las claves de cifrado que se han configurado en el Core.
- No hay límite en el número de claves de cifrado que pueden crearse en el Core.

Cómo agregar una clave de cifrado

Para agregar una clave de cifrado:

1. Vaya a Core Console.
2. Haga clic en **Configuration (Configuración)** → **Security (Seguridad)**.

   Se abrirá la página **Encryption (Cifrado)**.
3. Haga clic en **Actions (Acciones)** y, a continuación, haga clic en **Add Encryption Key (Agregar clave de cifrado)**.

   Se abrirá el cuadro de diálogo **Create Edit Encryption Key (Crear clave de cifrado)**.
4. En el cuadro de diálogo **Create Encryption Key (Crear clave de cifrado)**, introduzca los detalles para la clave según se describe a continuación:

Cuadro de texto	Descripción
Nombre	Introduzca un nombre para la clave de cifrado.

Cuadro de texto	Descripción
Descripción	Introduzca una descripción para la clave de cifrado. Se utiliza para proporcionar más detalles para la clave de cifrado.
Passphrase	Introduzca una frase de contraseña. Se utiliza para controlar el acceso.
Confirm Passphrase	Vuelva a introducir la frase de contraseña. Se utiliza para confirmar la entrada de la frase de contraseña.

5. Haga clic en **OK (Aceptar)**.

   PRECAUCIÓN: Se recomienda que proteja la frase de contraseña. Si pierde la frase de contraseña, no podrá acceder a los datos.

Edición de una clave de cifrado

Para editar una clave de cifrado:

1. Vaya a Core Console.
2. Haga clic en **Configuration (Configuración) → Security (Seguridad)**

   Se muestra la pantalla **Encryption Keys (Claves de cifrado)**.
3. Seleccione la clave de cifrado que desea modificar y haga clic en **Edit (Editar)**.

   Aparecerá el cuadro de diálogo **Edit Encryption Key (Editar clave de cifrado)**.
4. En el cuadro de diálogo **Edit Encryption Key (Editar clave de cifrado)**, edite el nombre o modifique la descripción de la clave de cifrado.
5. Haga clic en **OK (Aceptar)**.

Cómo cambiar la frase de contraseña de la clave de cifrado

Para cambiar la frase de contraseña de la clave de cifrado:

1. Vaya a Core Console.
2. Haga clic en **Configuration (Configuración) → Security (Seguridad)**.

   Se abrirá la página Encryption Keys (Claves de cifrado).
3. Seleccione la clave de cifrado que desea modificar y haga clic en **Change Passphrase (Cambiar frase de contraseña)**.

   Aparecerá el cuadro de diálogo **Change Passphrase (Cambiar frase de contraseña)**.
4. En el cuadro de diálogo **Change Passphrase (Cambiar frase de contraseña)**, escriba la nueva frase de contraseña de la Core y vuelva a escribirla para confirmarla.
5. Haga clic en **OK (Aceptar)**.

   PRECAUCIÓN: Se recomienda proteger la contraseña. Si la pierde, no podrá acceder a los datos del sistema.

Importación de una clave de cifrado

Para importar una clave de cifrado:

1. Vaya a Core Console.
2. Haga clic en **Configuration (Configuración) → Security (Seguridad)**.
3. Seleccione el menú desplegable **Actions (Acciones)** y, a continuación, haga clic en **Import (Importar)**.

Aparecerá el cuadro de diálogo **Import Key (Importar clave)**.

4. En el cuadro de diálogo **Import Key (Importar clave)**, haga clic en **Browse (Examinar)** para buscar la clave de cifrado que desea importar y, después, haga clic en **Open (Abrir)**.
5. Haga clic en **OK (Aceptar)**.

Exportación de una clave de cifrado

Para exportar una clave de cifrado:

1. Vaya a Core Console.
2. Haga clic en **Configuration (Configuración)** → **Security (Seguridad)**.
3. Haga clic en **>** junto al nombre de la clave de cifrado que desea exportar y, a continuación, haga clic en **Export (Exportar)**.

   Aparecerá el cuadro de diálogo **Export Key (Exportar clave)**.
4. En el cuadro de diálogo **Export Key (Exportar clave)**, haga clic en **Download Key (Descargar clave)** para guardar y almacenar las claves de cifrado en una ubicación segura.
5. Haga clic en **OK (Aceptar)**.

Eliminación de una clave de cifrado

Para eliminar una clave de cifrado:

1. Vaya a la Core Console.
2. Haga clic en **Configuration (Configuración)** → **Security (Seguridad)**.
3. Haga clic en **>** junto al nombre de la clave de cifrado que desea eliminar y, a continuación, haga clic en **Remove (Quitar)**.

   Aparecerá el cuadro de diálogo **Remove Key (Quitar clave)**.
4. En el cuadro de diálogo **Remove Key (Quitar clave)**, haga clic en **OK (Aceptar)** para eliminar la clave de cifrado.

   NOTA: Los datos no se descifran al eliminar una clave de cifrado.

Administración de cuentas de servicios en la nube

Su appliance DL le permite hacer una copia de seguridad de los datos mediante la creación de un archivo de copia de seguridad de los puntos de recuperación de una nube. Con su appliance DL, puede crear, editar y administrar su cuenta en la nube a través de un proveedor de almacenamiento en la nube. Puede archivar sus datos en la nube mediante servicios como Microsoft Azure, Amazon S3, Rackspace Cloud Block Storage u otros servicios en la nube basados en OpenStack. Consulte los temas siguientes para administrar sus cuentas de servicios en la nube:

- Cómo agregar una cuenta de servicios en la nube
- Edición de una cuenta de servicios en la nube
- Configuración de los valores de la cuenta de servicios en la nube
- Eliminación de una cuenta de servicios en la nube

Cómo agregar una cuenta de servicios en la nube

Antes de poder exportar los datos archivados con una nube, debe agregar la cuenta de su proveedor de servicios en la nube en la Core Console.

Para agregar una cuenta de servicios en la nube.

1. En la Core Console, haga clic en la pestaña **Tools (Herramientas)**.
2. En el menú de la izquierda, haga clic en **Clouds (Nubes)**.
3. En la página **Clouds (Nubes)**, haga clic en **Add New Account (Agregar cuenta nueva)**.
   Se abrirá el cuadro de diálogo **Add New Account (Agregar cuenta nueva)** .
4. En la lista desplegable **Cloud Type (Tipo de nube)**, seleccione un proveedor compatible de servicios en la nube.
5. Basándose en el tipo de nube que haya seleccionado en el paso 4, introduzca los detalles que se describen en la tabla siguiente.

Tipo de nube	Cuadro de texto	Descripción
Microsoft Azure	Storage Account Name (Nombre de cuenta de almacenamiento)	Escriba el nombre de la cuenta de almacenamiento de Windows Azure.
	Access Key (Clave de acceso)	Introduzca la clave de acceso de su cuenta.
	Display Name (Nombre de visualización)	Cree el nombre para mostrar de esta cuenta en AppAssure; por ejemplo, Windows Azure 1.
Amazon S3	Access Key (Clave de acceso)	Introduzca la clave de acceso de su cuenta de servicios de nube de Amazon.
	Secret Key (Clave secreta)	Escriba la clave secreta de esta cuenta.
	Display Name (Nombre de visualización)	Cree el nombre para mostrar de esta cuenta en AppAssure; por ejemplo, Amazon 1.
Con tecnología OpenStack	User Name (Nombre de usuario)	Escriba el nombre de usuario de su cuenta de servicios de nube en OpenStack.
	API Key (Clave API)	Escriba la clave API de su cuenta.
	Display Name (Nombre de visualización)	Cree el nombre para mostrar de esta cuenta en AppAssure; por ejemplo, OpenStack 1.
	Tenant ID (Id. de inquilino)	Escriba su Id. de inquilino para esta cuenta.
	Authentication URL (URL de autentificación)	Especifique la URL de autentificación para esta cuenta.

Tipo de nube	Cuadro de texto	Descripción
Cloud Block Storage de Rackspace	User Name (Nombre de usuario)	Escriba el nombre de usuario para la cuenta de servicios en la nube de Rackspace.
	API Key (Clave API)	Escriba la clave API de esta cuenta.
	Display Name (Nombre de visualización)	Cree el nombre para mostrar de esta cuenta en AppAssure; por ejemplo, Rackspace 1.

6. Haga clic en **Add (Agregar)**.
   El cuadro de diálogo se cierra y la cuenta se muestra en la página **Clouds (Nubes)** de la Core Console.

Edición de una cuenta de servicios en la nube

Realice los pasos siguientes para editar una cuenta de servicios en la nube:

1. En la Core Console, haga clic en la pestaña **Tools (Herramientas)**.
2. En el menú de la izquierda, haga clic en **Clouds (Nubes)**.
3. Junto a la cuenta de servicios en la nube que desea modificar, haga clic en el menú desplegable y, a continuación, haga clic en **Edit (Editar)**.
   Se abre la ventana **Edit Account (Editar cuenta)** .
4. Edite los detalles según sea necesario y, a continuación, haga clic en **Save (Guardar)**.

   NOTA: El tipo de nube no se puede editar.

Configuración de los valores de la cuenta de servicios en la nube

Los valores de configuración de la nube le permiten determinar la cantidad de veces que AppAssure debería intentar conectarse a su cuenta de servicios en la nube, y la cantidad de tiempo empleado en un intento antes de que se agote el tiempo de espera.
Para configurar los valores de la conexión de la cuenta de servicios en la nube:

1. En la Core Console, haga clic en la pestaña **Configuration (Configuración)**.
2. En el menú de la izquierda, haga clic en **Settings (Configuración)**.
3. En la página **Settings (Configuración)**, desplácese hacia abajo hasta la opción **Cloud Configuration (Configuración de la nube)**.
4. Haga clic en el menú desplegable junto a la cuenta de servicios en la nube que desee configurar y, a continuación, realice una de las acciones siguientes:
   - Haga clic en **Edit (Editar)**.
     Aparece el cuadro de diálogo **Cloud Configuration (Configuración de la nube)** .

     1. Utilice las teclas de flecha hacia arriba y hacia abajo para editar las opciones siguientes:

        – **Request Timeout (Tiempo de espera de solicitud):** Se muestra en minutos y segundos, determina la cantidad de tiempo que AppAssure debe invertir en cada intento para conectarse a la cuenta de servicios en la nube cuando hay un retraso. Los intentos de conexión cesarán después del lapso de tiempo especificado.

- **Retry Count (Número de reintentos):** Determina el número de intentos que AppAssure debe llevar a cabo antes de determinar que no se puede conectar con la cuenta de servicios en la nube.
- **Write Buffer Size (Tamaño del búfer de escritura):** Determina el tamaño del búfer que se reserva para escribir los datos archivados en la nube.
- **Read Buffer Size (Tamaño del búfer de lectura):** Determina el tamaño de bloque reservado para leer los datos archivados desde la nube.

2. Haga clic en **Next (Siguiente)**.

- Hacer clic en **Reset (Restablecer)** devuelve la configuración a los valores predeterminados siguientes:
  - **Request Timeout (Tiempo de espera de solicitud):** 01:30 (minutos y segundos)
  - **Retry Count (Número de reintentos):** 3 (intentos)

Eliminación de una cuenta de servicios en la nube

Puede eliminar una cuenta de servicios en la nube, interrumpir el servicio en la nube o dejar de usarla para un Core determinado.
Para eliminar una cuenta de servicios en la nube:

1. En la Core Console, haga clic en la ficha **Tools (Herramientas)**.
2. En el menú de la izquierda, haga clic en **Clouds (Nubes)**.
3. Junto a la cuenta de servicios en la nube que desea editar, haga clic en el menú desplegable y, a continuación, haga clic en **Remove (Quitar)**.
4. En la ventana **Delete Account (Eliminar cuenta)**, haga clic en **Yes (Sí)** para confirmar que desea eliminar la cuenta.
5. Si la cuenta de servicios en la nube está actualmente en uso, en una segunda ventana se le preguntará si desea eliminarla. Haga clic en **Yes (Sí)** para confirmar.

   NOTA: La eliminación de una cuenta que está actualmente en uso hace que fallen todos los trabajos de archivo programados para esa cuenta.

Comprensión de la replicación

Acerca de la protección de estaciones de trabajo y servidores

Para proteger sus datos agregue las estaciones de trabajo y los servidores que desea proteger en la Core Console; por ejemplo, el servidor de Exchange, SQL Server o el servidor de Linux.

NOTA: En este capítulo, el término *máquina* también se refiere en general al software del Agent instalado en esa máquina.

En la Core Console, puede identificar la máquina en la que está instalado un Agent y especificar qué volúmenes proteger, definir programas para la protección, agregar medidas de seguridad adicionales como el cifrado, etc. Para obtener más información sobre cómo acceder a la Core Console para proteger estaciones de trabajo y servidores, consulte Cómo proteger una máquina.

Acerca de la replicación

La replicación es el proceso de copiar puntos de recuperación y transferirlos a una ubicación secundaria para la recuperación ante desastres. El proceso de replicación requiere una relación de emparejamiento de origen-destino entre dos Cores. El Core de origen copia los puntos de recuperación de los Agents protegidos y, a continuación, los transfiere de forma continua y asíncrona a un Core de destino en un sitio remoto de recuperación ante desastres. La ubicación externa puede ser un centro de datos

propiedad de la empresa (Core administrado automáticamente) o una ubicación o entorno de nube del proveedor de servicio (MSP) administrado por un tercero. Cuando replique a un MSP, puede usar flujos de trabajo integrados que le permiten solicitar conexiones y recibir notificaciones de comentarios automáticas. Estos son algunos escenarios de replicación posibles:

- **Replication to a Local Location (Replicación a una ubicación local)**. El Core de destino se encuentra en un centro de datos local o en una ubicación remota y la replicación se mantiene en todo momento. En esta configuración, la pérdida del Core no impide una recuperación.
- **Replication to an Off-site Location (Replicación a una ubicación externa)**. El Core de destino se encuentra en unas instalaciones de recuperación ante desastres externas para la recuperación en caso de pérdida.
- **Mutual Replication (Replicación mutua)**. Dos centros de datos en dos ubicaciones diferentes contienen un Core cada uno, protegen los Agents y sirven como copia de seguridad para recuperación de desastres externa entre sí. En este escenario, cada Core replica los Agents en el Core ubicado en el otro centro de datos.
- **Hosted and Cloud Replication (Replicación alojada y en la nube)**. Los socios de AppAssure MSP mantienen múltiples Cores de destino en un centro de datos o en una nube pública. En cada uno de estos Cores, el socio MSP permite a uno o más de sus clientes replicar puntos de recuperación desde un Core de origen en el sitio del cliente hasta el Core de destino del MSP por una cuota.

  NOTA: En este escenario, los clientes solo tienen acceso a sus propios datos.

Estas son algunas de las configuraciones posibles de replicación:

- **Point to Point (Punto a punto)**. Replica un único Agent desde un Core de origen único a un Core de destino único.

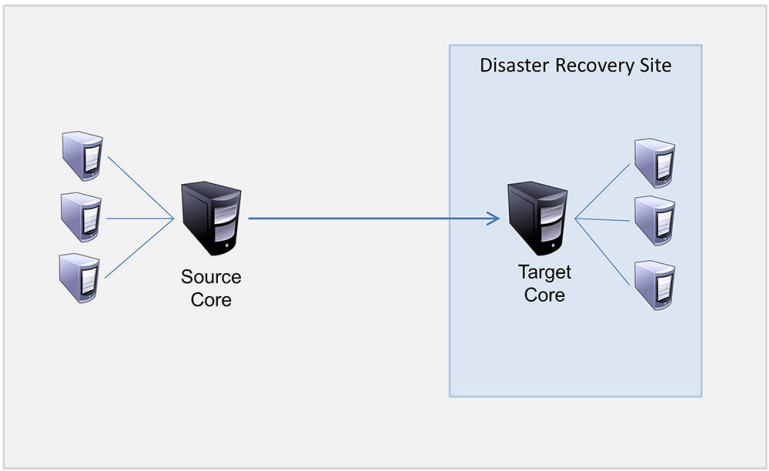

Ilustración 7. Diagrama de la arquitectura de replicación básica

- **Multi-Point to Point (Multipunto a punto)**. Replica varios Cores de origen a un solo Core de destino.

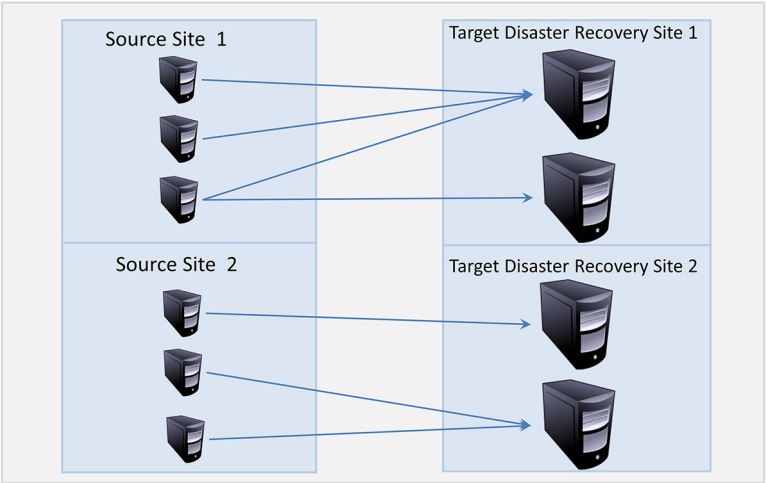

Ilustración 8. Diagrama de la arquitectura de replicación multipunto

Acerca de la inicialización

La replicación se inicia con la inicialización: la transferencia inicial de imágenes base desduplicadas e instantáneas incrementales de los Agents protegidos, que pueden llegar a totalizar hasta cientos o miles de gigabytes de datos. La replicación inicial puede inicializarse hasta el Core de destino mediante el uso de medios externos para transferir los datos iniciales al Core de destino. Esto normalmente es útil para grandes conjuntos de datos o sitios con enlaces lentos.

NOTA: Aunque es posible inicializar los datos base a través de una conexión de red, no se recomienda hacerlo. La inicialización inicial implica normalmente cantidades de datos enormes, que podrían superar las capacidades de una conexión WAN típica. Por ejemplo, si los datos de inicialización alcanzan la cantidad de 10 GB y el enlace WAN transfiere 24 Mbps, la transferencia puede requerir más de 40 días en completarse.

Los datos en el archivo de inicialización están comprimidos, cifrados y desduplicados. Si el tamaño total del archivo es mayor que el espacio disponible en los medios extraíbles, el archivo puede distribuirse entre varios dispositivos en función del espacio disponible en los medios. Durante el proceso de inicialización, se replican los puntos de recuperación en el sitio de destino. Cuando el Core de destino consume el archivo de inicialización, los puntos de recuperación incrementales recién replicados se sincronizan automáticamente.

El proceso de inicialización tiene dos partes (también denominadas copiar-consumir):

- La primera parte implica copiar, que es la escritura de los datos replicados iniciales a una fuente de medios extraíbles. Copiar duplica todos los puntos de recuperación existentes desde el Core de origen hasta un dispositivo de almacenamiento extraíble local, como por ejemplo una unidad USB. Cuando la copia finalice, deberá transportar la unidad desde la ubicación del Core de origen hasta la ubicación del Core de destino.
- La segunda parte es consumir, que se produce cuando un Core de destino recibe la unidad transportada y copia los datos replicados en el repositorio. A continuación, el Core de destino consume los puntos de recuperación y los utiliza para formar Agents replicados.

NOTA: Aunque se puede producir la replicación de instantáneas incrementales entre los Cores de origen y destino antes de que se complete la inicialización, las instantáneas replicadas que se transmiten del origen al destino quedarán "huérfanas" hasta que se consuman los datos iniciales y se combinen con las imágenes base replicadas.

Como hay que copiar grandes cantidades de datos al dispositivo de almacenamiento portátil, se recomienda usar una conexión eSATA, USB 3.0 y otra de alta velocidad con el dispositivo de almacenamiento portátil.

Acerca de la conmutación por error y la conmutación por recuperación

En caso de grave interrupción en la que fallen el Core de origen y los Agents, su servidor DL admite conmutación por error y conmutación por recuperación en entornos replicados. La conmutación por error consiste en cambiar a un Core de destino redundante o en espera al producirse un error del sistema o una terminación anormal de un Core de origen y de los Agents asociados. El objetivo principal de la conmutación por error es iniciar un nuevo Agent idéntico al Agent en error protegido por el Core de origen en error. El objetivo secundario es cambiar el Core de destino a un nuevo modo para que el Core de destino proteja al Agent de conmutación por error de la misma forma que el Core de origen protegía al Agent inicial antes del error. El Core de destino podrá recuperar instancias de los Agents replicados y comenzar inmediatamente la protección en las máquinas con conmutación por error.

La conmutación por recuperación es el proceso de restaurar un Agent y un Core a sus estados originales (antes del fallo). El objetivo principal de la conmutación por recuperación es restaurar el Agent (en la mayoría de los casos, se trata de una nueva máquina que reemplaza a un Agent fallido) a un estado idéntico al último estado del nuevo Agent temporal. Al restaurarse, queda protegido por un Core de origen restaurado. La replicación también se restaura y el Core de destino actúa de nuevo como destino de replicación.

Acerca de la replicación y los puntos de recuperación cifrados

Aunque la unidad de inicialización no contiene copias de seguridad del registro y certificados del Core de origen, la unidad de inicialización contiene claves de cifrado del Core de origen si los puntos de recuperación replicados desde el Core de origen están cifrados. Los puntos de recuperación replicados se mantienen cifrados después de su transmisión hasta el Core de destino. Los propietarios o administradores del Core de destino necesitan la frase de contraseña para recuperar los datos cifrados.

Acerca de las políticas de retención para replicación

La política de retención en el Core de origen determina la política de retención para los datos replicados al Core de destino, porque la tarea de replicación transmite los puntos de recuperación fusionados que se producen a partir de un mantenimiento periódico o eliminación ad-hoc.

NOTA: El Core de destino no puede realizar un mantenimiento periódico o eliminar ad-hoc de puntos de recuperación. Estas acciones solo puede realizarlas el Core de origen.

Consideraciones de rendimiento para la transferencia de datos replicados

Si el ancho de banda entre el Core de origen y el Core de destino no puede alojar la transferencia de los puntos de recuperación almacenados, la replicación empezará con la inicialización del Core de destino con imágenes base y puntos de recuperación de los servidores seleccionados protegidos en el Core de origen. El proceso de inicialización solo se tiene que realizar una vez, ya que sirve como base necesaria para la replicación programada regularmente.

Cuando se prepare para la replicación, debería tener en cuenta los factores siguientes:

Velocidad de cambio	La velocidad de cambio es la velocidad a la que se acumula la cantidad de datos protegidos. La velocidad depende de la cantidad de datos que cambia en los volúmenes protegidos y del intervalo de protección de los volúmenes. Si cambia

un conjunto de bloques del volumen, reducir el intervalo de protección reducirá la velocidad de cambio.

Ancho de banda

El ancho de banda es la velocidad de transferencia disponible entre el Core de origen y el Core de destino. Es crucial que el ancho de banda sea mayor que la velocidad de cambio para que la replicación siga el ritmo de los puntos de recuperación creados por las instantáneas. Debido a la cantidad de datos transmitidos de Core a Core, puede que sean necesarias varias secuencias paralelas para funcionar a velocidades de cable de hasta la velocidad de una conexión Ethernet de 1 GB.

NOTA: El ancho de banda especificado por el ISP es el ancho de banda disponible total. El ancho de banda saliente es compartido por todos los dispositivos de la red. Asegúrese de que haya suficiente ancho de banda libre para que la replicación aloje la velocidad de cambio.

Número de Agents

Es importante tener en cuenta el número de Agents protegidos por Core de origen y cuántos tiene pensado replicar en el destino. AppAssure le permite realizar la replicación por servidor protegido, así que puede elegir replicar determinados servidores. Si todos los servidores protegidos deben replicarse, esto afectará de forma considerable a la velocidad de cambio, en especial si el ancho de banda entre los Cores de origen y de destino no es suficiente para la cantidad y el tamaño de los puntos de recuperación que se estén replicando.

Según su configuración de red, la replicación puede ser un proceso muy largo.

La siguiente tabla muestra ejemplos del ancho de banda necesario por gigabyte para una velocidad de cambio razonable

NOTA: Cumpla las recomendaciones que se enumeran en la siguiente tabla para obtener resultados óptimos.

Tabla 1. Velocidad de cambio máxima para tipos de conexión WAN

Banda ancha	Ancho de banda	Velocidad máxima de cambio
DSL	768 Kbps y superior	330 MB por hora
Cable	1 Mbps y superior	429 MB por hora
T1	1,5 Mbps y superior	644 MB por hora
Fibra	20 Mbps y superior	838 GB por hora

Si un enlace falla durante la transferencia de datos, la replicación se reanuda desde el punto de error anterior de la transferencia después de que se restaure el enlace funcionalmente.

Plan para realizar la replicación

Para replicar los datos mediante AppAssure, debe configurar los Cores de origen y de destino para la replicación. Después de configurar la replicación, puede replicar los datos del Agent, supervisar y administrar la replicación y realizar la recuperación.

La replicación en AppAssure implica realizar las operaciones siguientes:

- Configurar la replicación administrada automáticamente. Para obtener más información acerca de cómo replicar a un Core de destino administrado automáticamente, consulte Replicación a un Core administrado automáticamente.
- Configurar la replicación de terceros. Para obtener más información acerca de cómo replicar a un Core de destino de terceros, consulte Replicación a un Core administrado por un tercero
- Replicar un Agent nuevo conectado al Core de origen. Para obtener más información acerca de cómo replicar un Agent, consulte Replicación de un Agent nuevo.
- Replicar un Agent existente. Para obtener más información sobre la configuración de un Agent para la replicación, consulte Replicación de los datos de un Agent en una máquina.
- Establecer la prioridad de replicación para un Agent. Para obtener más información sobre cómo priorizar la replicación de los Agents, consulte Configuración de la prioridad de replicación para un Agent.
- Supervisar la replicación según sea necesario. Para obtener más información sobre cómo supervisar la replicación, ver Monitoring Replication (Supervisión de la replicación).
- Administrar la configuración de replicación según sea necesario. Para obtener más información acerca de cómo administrar la configuración de replicación, consulte Administración de configuraciones de replicación.
- Recuperar los datos replicados ante situaciones de desastre o pérdida de datos. Para obtener más información acerca de cómo recuperar datos replicados, consulte Recuperación de datos replicados .

Replicación a un Core administrado automáticamente

Un Core administrado automáticamente es aquel al que tiene acceso, generalmente porque lo administra su compañía en otra ubicación. La replicación se puede completar totalmente en el Core de origen, a menos que decida inicializar los datos. La inicialización requiere consumir la unidad de inicialización en el Core de destino después de configurar la replicación en el Core de origen.

NOTA: Esta configuración se aplica a la replicación en una ubicación externa y a la replicación mutua. El Core se debe instalar en todas las máquinas de origen y de destino. Si está configurando su sistema para la replicación multipunto a punto, debe realizar esta tarea en todos los Cores de origen y en el Core de destino.

Configuración del Core de origen para replicar a un Core de destino administrado automáticamente

Para configurar el Core de origen para replicar a un Core de destino administrado automáticamente:

1. En la Core Console, haga clic en la pestaña **Replication (Replicación)**.
2. Haga clic en **Add Target Core (Agregar Core de destino)**.
   Se abrirá el asistente **Replication (Replicación)**.
3. Seleccione **I have my own Target Core (Tengo mi propio Core de destino)** y, a continuación, introduzca la información según se describe en la tabla siguiente.

Cuadro de texto	Descripción
Host Name (Nombre del host)	Introduzca el nombre de host o dirección IP de la máquina del Core en la que esté replicando.
Port (Puerto)	Introduzca el número de puerto con el que el AppAssure Core se comunica con la máquina. El número de puerto predeterminado es 8006.

Cuadro de texto	Descripción
User Name (Nombre de usuario)	Introduzca el nombre de usuario para acceder a la máquina. Por ejemplo, **Administrador.**
Passsword (Contraseña)	Introduzca la contraseña para acceder a la máquina.

Si el Core que desea agregar se ha emparejado anteriormente con este Core de origen, lleve a cabo los pasos siguientes:

a. Seleccione **Use an existing target core (Usar un Core de destino existente)**.
b. En la lista desplegable, seleccione el Core de destino.
c. Haga clic en **Next (Siguiente)**.
d. Vaya al paso 7.

4. Haga clic en **Next (Siguiente)**.
5. En la página **Details (Detalles)**, especifique un nombre para esta configuración de replicación; por ejemplo, SourceCore1. Si está volviendo a iniciar o reparando una configuración de replicación anterior, seleccione **My Core has been migrated and I would like to repair replication (Se ha migrado el Core y me gustaría reparar la replicación).**
6. Haga clic en **Next (Siguiente)**.
7. En la página **Agents (Agentes)**, elija los Agents que desea replicar y, a continuación, utilice las listas desplegables de la columna **Repository (Repositorio)** y seleccione un repositorio para cada Agent.
8. Si tiene pensado realizar el proceso de inicialización para la transferencia de los datos de la base, lleve a cabo los pasos siguientes:

   NOTA: Como hay que copiar grandes cantidades de datos al dispositivo de almacenamiento portátil, se recomienda usar una conexión eSATA, USB 3.0 y otra de alta velocidad con el dispositivo de almacenamiento portátil.

   a. En la página **Agents (Agentes)**, seleccione **Use a seed drive to perform initial transfer (Utilizar una unidad de inicialización para realizar la transferencia inicial)**. Si actualmente se están replicando uno o más Agents en un Core de destino, para incluir esos Agents en la unidad de inicialización seleccione **With already replicated (Con los ya replicados)**.
   b. Haga clic en **Next (Siguiente)**.
   c. En la página **Seed Drive Location (Ubicación de la unidad de inicialización)**, utilice la lista desplegable **Location type (Tipo de ubicación)** para seleccionar una de las opciones siguientes:
      - Local: en el cuadro de texto **Location (Ubicación)**, especifique dónde desea guardar la unidad de inicialización; por ejemplo, D:\trabajo\archivo.
      - Network (Red): en el cuadro de texto **Location (Ubicación)**, especifique dónde desea guardar la unidad de inicialización y, a continuación, introduzca sus credenciales del recurso compartido de red en los cuadros de texto **User name (Nombre de usuario)** y **Password (Contraseña)**.
      - Cloud (Servicios en la nube): en el cuadro de texto **Account (Cuentas)** , seleccione la cuenta. Para seleccionar una cuenta de servicios en la nube, debe haberla agregado primero en la Core Console. Para obtener más información, consulte Cómo agregar una cuenta de servicios en la nube. Seleccione el **Container (Contenedor)** asociado con su cuenta. Seleccione el **Folder Name (Nombre de la carpeta)** donde guardará los datos archivados.
   d. Haga clic en **Next (Siguiente)**.
9. En el cuadro de diálogo **Seed Drive Option (Opciones de la unidad de inicialización)**, introduzca la información que se describe a continuación:

Cuadro de texto	Descripción
Maximun Size (Tamaño máximo)	Los grandes archivos de datos pueden dividirse en múltiples segmentos. Seleccione el tamaño máximo del segmento que desea reservar para crear la unidad de inicialización mediante una de las acciones siguientes: • Seleccione **Entire Target (Todo el destino)** para reservar todo el espacio disponible en la ruta de acceso proporcionada en la página Seed Drive Location (Ubicación de la unidad de inicialización) para su uso en el futuro (por ejemplo, si la ubicación es D:\trabajo\archivo, se reservará todo el espacio disponible en la unidad D: por si es necesario para copiar la unidad de inicialización, pero no se reserva inmediatamente después de iniciar el proceso de copia). • Seleccione el cuadro de texto en blanco, introduzca una cantidad y, a continuación, seleccione una unidad de medida en la lista desplegable para personalizar el espacio máximo que desea reservar.
Customer ID (Id. de cliente) (opcional)	Opcionalmente, introduzca la Id. del cliente que le asignó el proveedor de servicio.
Recycle action (Acción de reciclaje)	En el caso de que la ruta de acceso ya contenga una unidad de inicialización, seleccione una de las opciones siguientes: • **Do not reuse (No reutilizar)**: no sobrescribe ni borra los datos existentes de la ubicación. Si la ubicación no está vacía, fallará la escritura de la unidad de inicialización. • **Replace this core (Reemplazar este Core)**:sobrescribe los datos que ya existen y que pertenecen a este Core, pero deja intactos los datos de los otros Cores. • **Erase completely (Borrar completamente)**: borra todos los datos del directorio antes de escribir la unidad de inicialización.
Comment (Comentario)	Introduzca un comentario o una descripción del archivo.
Add all Agents to Seed Drive (Agregar todos los agents a la unidad de inicialización)	Seleccione los Agents que desea replicar utilizando la unidad de inicialización.
Build RP chains (fix orphans) (Compilar cadena de PR [arreflar huérfanos])	Seleccione esta opción para replicar toda la cadena de puntos de recuperación (PR) en la unidad de inicialización. Esta opción está seleccionada de manera predeterminada. En AppAssure, la inicialización típica replica solo el último punto de recuperación a la unidad de inicialización, lo que reduce la cantidad de tiempo y espacio necesario para crear la unidad de inicialización. La opción para crear cadenas de punto de recuperación para la unidad de inicialización requiere el espacio suficiente en esa unidad para almacenar los puntos de recuperación más recientes desde uno o varios Agents especificados, lo cual puede llevar un tiempo adicional para completar la tarea.

Cuadro de texto	Descripción
Use compatible format (Usar formato compatible)	Seleccione esta opción para crear la unidad de inicialización en un formato que sea compatible con las versiones nuevas y anteriores de AppAssure Core.

10. En la página **Agents (Agentes)**, seleccione los Agents que desea replicar en el Core de destino usando la unidad de inicialización.
11. Haga clic en **Finish (Finalizar)**.
12. Si ha creado una unidad de inicialización, envíela al Core de destino.

    El emparejamiento del Core de origen con el Core de destino ha finalizado. La replicación se inicia, pero produce puntos de recuperación huérfanos en el Core de destino hasta que la unidad de inicialización se consume y proporciona las imágenes base.

Consumo de la unidad de inicialización en un Core de destino

Este procedimiento solo es necesario si creó una unidad de inicialización durante la Configuración de la replicación de un Core administrado automáticamente.
Para consumir una unidad de inicialización en un Core de destino:

1. Si la unidad de inicialización se guardó en un dispositivo de almacenamiento portátil como una unidad USB, conecte la unidad al Core de destino.
2. Desde la Core Console en el Core de origen, seleccione la pestaña **Replication (Replicación)**.
3. En **Incoming Replication (Replicación entrante)**, seleccione el Core de origen correcto en el menú desplegable y, a continuación, haga clic en **Consume (Consumir)**.

   Aparece la ventana Consume (Consumir).
4. Para **Location Type (Tipo de ubicación)**, seleccione una de las opciones siguientes en la lista desplegable:
   - Local
   - Network (Red)
   - Cloud (Nube)
5. Introduzca la información siguiente según sea necesario:

Cuadro de texto	Descripción
Location (Ubicación)	Introduzca la ruta de acceso de la unidad de inicialización, como una unidad USB o un recurso compartido de red (por ejemplo, D:\).
Username (Nombre de usuario)	Introduzca el nombre de usuario de la carpeta o unidad compartida. El nombre de usuario solo se requiere para una ruta de acceso de red.
Password (Contraseña)	Introduzca la contraseña de la carpeta o unidad compartida. La contraseña solo se requiere para una ruta de acceso de red.
Account (Cuenta)	Seleccione una cuenta desde la lista desplegable. Para seleccionar una cuenta de servicios en la nube, debe haberla agregado primero en la Core Console.
Container (Contenedor)	En el menú desplegable, seleccione un contenedor asociado con la cuenta.

Cuadro de texto	Descripción
Folder Name (Nombre de carpeta)	Introduzca el nombre de la carpeta en la que se guarda los datos archivados; por ejemplo, -Archivo- [FECHA DE CREACIÓN] - [TIEMPO DE CREACIÓN]

6. Haga clic en **Check File (Comprobar archivo)**.

   Una vez que el Core comprueba el archivo, rellena automáticamente el campo **Date Range (Rango de fechas)** con las fechas de los puntos de recuperación más antiguos y más recientes incluidos en la unidad de inicialización. También importa los comentarios introducidos en Configuración de la replicación de un Core administrado automáticamente.
7. En **Agent Names (Nombres de Agent)** en la ventana **Consume (Consumir)**, seleccione las máquinas para las que desea consumir datos y, a continuación, haga clic en **Consume (Consumir)**.

   NOTA: Para supervisar el progreso de consumo de datos, seleccione la pestaña **Events (Eventos)**.

Abandono de una unidad de inicialización pendiente

Si crea una unidad de inicialización con la intención de consumirla en el Core de destino, pero decide no enviarla a la ubicación remota, el enlace a dicha unidad de inicialización pendiente permanecerá en la pestaña **Replication (Replicación)** del Core de origen. Puede abandonar la unidad de inicialización pendiente para dar prioridad a datos de inicialización diferentes o más actualizados.

NOTA: Mediante este proceso, se elimina la unidad de inicialización pendiente de la Core Console en el Core de origen, pero no se elimina la unidad de la ubicación de almacenamiento en la que se guardó.

Para abandonar una unidad de inicialización pendiente:

1. En la Core Console en el Core de origen, seleccione la pestaña **Replication (Replicación)**.
2. Haga clic en **Outstanding Seed Drive (#) (N.º de unidades de inicialización pendientes)**.

   Aparecerá la sección **Outstanding seed drives (Unidades de inicialización pendientes)**, que muestra el nombre del Core de destino remoto, la fecha y hora en las que se creó la unidad de inicialización y el intervalo de datos de los puntos de recuperación incluidos en la unidad.
3. Haga clic en el menú desplegable de la unidad que desea abandonar y elija **Abandon (Abandonar)**.

   Aparecerá la ventana **Outstanding Seed Drive (Unidad de inicialización pendiente)**.
4. Haga clic en **Yes (Sí)** para confirmar la acción.

   La unidad de inicialización se eliminará. Si no hay más unidades de inicialización en el Core de origen, la próxima vez que abra la pestaña **Replication (Replicación)**, no aparecerá el enlace **Outstanding Seed Drive (#) (N.º de unidades de inicialización pendientes)** ni la sección **Outstanding seed drives (Unidades de inicialización pendientes)**.

Replicación a un Core administrado por un tercero

Un Core de terceros es un Core de destino que un MSP se encarga de administrar y mantener. Para replicar a un Core administrado por terceros no es necesario tener acceso al Core de destino. Una vez que un cliente configura la replicación en el Core o los Cores de destino, el MSP finaliza la configuración en el Core de destino.

NOTA: Esta configuración se aplica a la replicación alojada y en la nube. El AppAssure Core debe estar instalado en todas las máquinas Core de origen.

Configuración de la replicación a un Core de destino administrado por un tercero

NOTA: Esta configuración se aplica a la replicación alojada y en la nube. Si va a configurar AppAssure para la replicación multipunto a punto, realice esta tarea en todos los Cores de origen.

Para configurar la replicación de un Core administrado por un tercero:

1. Vaya a la Core Console y haga clic en la pestaña **Replication (Replicación)**.
2. En el menú desplegable **Actions (Acciones)**, haga clic en **Add Remote Core (Agregar Core remoto)**.
3. En el cuadro de diálogo **Select Replication Type (Seleccionar tipo de replicación)**, seleccione la opción **I have a subscription to a third-party providing off-site backup and disaster recovery services, and wish to replicate my backups to that service (Tengo una suscripción a un tercero que proporciona servicios de copia de seguridad y recuperación tras desastres remotos y deseo replicar mis copias de seguridad en este servicio)** y, después, introduzca la información, según se describe a continuación:

Cuadro de texto	Descripción
Nombre del host	Introduzca el nombre de host, dirección IP o FQDN para la máquina del Core remoto.
Port	Introduzca el número de puerto que le indicó el proveedor de servicios de terceros. El número de puerto predeterminado es 8006.

4. Haga clic en **Continue (Continuar)**.
5. En el cuadro de diálogo **Add Remote Core (Agregar Core remoto)**, haga lo siguiente:
   a. Seleccione los Agents que replicar.
   b. Seleccione un repositorio para cada Agent.
   c. Escriba la dirección de correo electrónico de la suscripción y el Id. de cliente que le proporcionó el proveedor de servicios.
6. Si tiene pensado realizar el proceso de inicialización para la transferencia de los datos de base, seleccione **Use a seed drive to perform initial transfer (Utilizar una unidad de inicialización para realizar la transferencia inicial)**.
7. Haga clic en **Submit Request (Enviar solicitud)**.

   NOTA: Si ha seleccionado la opción **Use a seed drive to perform initial transfer (Utilizar una unidad de inicialización para realizar una transferencia inicial)**, se mostrará el cuadro de diálogo **Copy to Seed Drive (Copiar en unidad de inicialización)**.
8. En el cuadro de diálogo **Copy to Seed Drive (Copiar en unidad de inicialización)**, introduzca la información para la unidad de inicialización, según se describe en la siguiente tabla.

Cuadro de texto	Descripción
Ubicación	Introduzca la ruta de acceso a la unidad en la que desea guardar los datos iniciales, por ejemplo, en la unidad USB local.
Nombre de usuario	Introduzca el nombre del usuario para conectar a la unidad. NOTA: Esto es necesario si la unidad de inicialización se encuentra en un recurso compartido de red.
Contraseña	Introduzca la contraseña para conectarse a la unidad.

Cuadro de texto	Descripción
	NOTA: Esto es necesario si la unidad de inicialización se encuentra en un recurso compartido de red.
Maximum size (Tamaño máximo)	Seleccione una de las opciones siguientes: • El destino completo. • Una parte del espacio disponible de la unidad. Para designar una parte de la unidad: a. Introduzca la cantidad de espacio deseada en el cuadro de texto. b. Seleccione la medida.
Recycle action (Acción de reciclaje)	En el caso de que la ruta de acceso ya contenga una unidad de inicialización, seleccione una de las opciones siguientes: • **Do not reuse (No reutilizar)**: no sobrescribe ni borra los datos existentes de la ubicación. Si la ubicación no está vacía, fallará la escritura de la unidad de inicialización. • **Replace this core (Reemplazar este Core)**:sobrescribe los datos que ya existen y que pertenecen a este Core, pero deja intactos los datos de los otros Cores. • **Erase completely (Borrar completamente)**: borra todos los datos del directorio antes de escribir la unidad de inicialización.
Comment	Introduzca un comentario o una descripción del archivo.
Agents	Seleccione los Agents que desea replicar utilizando la unidad de inicialización.

NOTA: Como hay que copiar grandes cantidades de datos al dispositivo de almacenamiento portátil, se recomienda usar una conexión eSATA, USB 3.0 y otra de alta velocidad con el dispositivo de almacenamiento portátil.

9. Haga clic en **Start (Iniciar)** para escribir la unidad de inicialización en la ruta de acceso que haya proporcionado.
10. Envíe la unidad de inicialización según lo indicado por el proveedor de servicios de terceros.

Revisión de una solicitud de replicación

Se envía una solicitud de replicación desde el Core de origen hasta el Core de destino de terceros. Como tercero, usted puede revisar la solicitud y aprobarla para iniciar la replicación para su cliente, o también puede rechazarla para evitar que se produzca la replicación.

Para revisar una solicitud de replicación en un Core de destino de terceros:

1. Abra la Core Console en el Core de destino y haga clic en la pestaña **Replication (Replicación)**.
2. Haga clic en **Pending Requests (#) (N.º de solicitudes pendientes)**.
   Aparece la sección **Pending Replication Requests (Solicitudes de replicación pendientes)**.
3. Junto a la solicitud que desea revisar, seleccione **Review (Revisar)** en el menú desplegable.
   Aparecerá la ventana **Review Replication Request (Revisar solicitud de replicación)**.

NOTA: La solicitud rellenada por el cliente establece la información que aparece en la sección **Source Core Identity (Identidad del Core de origen)**.

4. En la ventana Review Replication Request (Revisar solicitud de replicación), realice una de las acciones siguientes:
   - Para rechazar la solicitud, haga clic en **Deny (Denegar)**.
   - Para aprobar la solicitud:
     1. – Seleccione **Replace an existing replicated Core (Reemplazar un Core replicado existente)**y, a continuación, seleccione un Core en la lista desplegable.
        – Seleccione **Create a new source Core (Crear un nuevo Core de origen)**. Compruebe los campos **Core Name (Nombre de Core)**, **Email Address (Dirección de correo electrónico)** del cliente y **Customer ID (Id. de cliente)**, y edite la información según proceda.
     2. Bajo **Agents**, seleccione las máquinas a las que se va a aplicar la aprobación y, a continuación, seleccione el repositorio adecuado para cada máquina en la lista desplegable.
     3. De manera opcional, introduzca las notas que desea que aparezcan en el cuadro **Comment (Comentario)**.
     4. Haga clic en **Send Response (Enviar respuesta)**.

        La replicación se habrá aceptado.

Omisión de una solicitud de replicación

Como proveedor de servicios de terceros de un Core de destino, tiene la opción de ignorar una solicitud de replicación enviada por un cliente. Esta opción se puede usar cuando un cliente envía una solicitud por error o si desea rechazar una solicitud sin revisarla primero.

Para omitir una solicitud de replicación:

1. Desde la Core Console en el Core de origen, seleccione la pestaña **Replication (Replicación)**.
2. En la pestaña de replicación, haga clic en **Pending Requests (#) (N.º de solicitudes pendientes)**.
   Aparece la sección **Pending Replication Requests (Solicitudes de replicación pendientes)**.
3. Junto a la solicitud que desea omitir, seleccione **Ignore (Omitir)** en el menú desplegable.
   El Core de destino envía una notificación al Core de origen indicando que la solicitud se ha omitido.

Supervisión de la replicación

Cuando la replicación esté configurada, puede supervisar el estado de las tareas de replicación para los Cores de origen y destino. Puede actualizar la información del estado, ver detalles de replicación, etc.

Para supervisar la replicación

1. En la Core Console, haga clic en la pestaña **Replication (Replicación)**.
2. En esta pestaña, puede ver información y supervisar el estado de las tareas de replicación, según se describe a continuación:

Sección	Descripción	Acciones disponibles
Pending Replication Requests (Solicitudes de replicación pendientes)	Muestra el Id. de cliente, la dirección de correo electrónico y el nombre del host cuando se envía una solicitud de replicación a un proveedor de servicios de terceros. Aparece	En el menú desplegable, haga clic en **Ignore (Omitir)** para omitir o rechazar la solicitud.

Sección	Descripción	Acciones disponibles
	en esta sección hasta que MSP acepta la solicitud.	
Outstanding Seed Drives (Unidades de inicialización pendientes)	Enumera las unidades de inicialización que se han escrito pero que el Core de destino aún no ha consumido. Incluye el nombre de Core remoto, la fecha de creación y el intervalo de fechas.	En el menú desplegable, haga clic en **Abandon (Abandonar)** para abandonar o cancelar el proceso de inicialización.
Outgoing Replication (Replicación de salida)	Enumera todos los Cores de destino en los que se replica el Core de origen. Incluye el nombre del Core remoto, el estado de existencia, el número de máquinas Agent a replicar y el progreso de una transmisión de replicación.	En un Core de origen, en el menú desplegable, puede seleccionar las opciones siguientes: • **Details (Detalles)**: muestra el Id., URI, nombre de visualización, estado, Id. de cliente, dirección de correo electrónico y comentarios del Core replicado. • **Change Settings (Cambiar configuración)**: enumera el nombre de visualización y le permite editar el host y puerto para el Core de destino. • **Add Agents (Agregar Agents)**: le permite elegir un host de una lista desplegable, seleccionar Agents protegidos para replicación y crear una unidad de inicialización para la transferencia inicial del Agent nuevo.
Incoming Replication (Replicación entrante)	Enumera todas las máquinas de origen desde las que el destino recibe datos replicados. Incluye el nombre del Core remoto, estado, máquinas y progreso.	En un Core de destino, en el menú desplegable, puede seleccionar las opciones siguientes: • **Details (Detalles)**: muestra el Id., nombre de host, Id. de cliente, dirección de correo electrónico y comentarios del Core replicado. • **Consume (Consumir)**: consume los datos iniciales de la unidad de inicialización y los guarda en el repositorio local.

3. Haga clic en el botón **Refresh (Actualizar)** para actualizar las selecciones de esta pestaña con la información más reciente.

Administración de configuraciones de replicación

Puede ajustar una serie de configuraciones para la forma en la que se ejecuta la replicación en los Cores de origen y destino.

Para administrar las configuraciones de replicación:

1. En la Core Console, haga clic en la pestaña **Replication (Replicación)**.
2. En el menú desplegable **Actions (Acciones)**, haga clic en **Settings (Configuración)**.
3. En la ventana **Replication Settings (Configuración de replicación)**, edite la configuración de replicación, según se describe a continuación:

Opción	Descripción
Cache lifetime (Vida útil de la caché)	Especifica el tiempo entre las solicitudes de estado de Core de destino realizadas por el Core de origen.
Volume image session timeout (Tiempo de espera de sesión de imagen de volumen)	Especifica el tiempo que el Core de origen tarda en intentar transferir una imagen de volumen al Core de destino.
Max. concurrent replication jobs (Trabajos de replicación concurrentes máx.)	Especifica el número de Agents que tienen permiso para replicar a la vez en el Core de destino.
Max. parallel streams (Transmisiones en paralelo máx.)	Especifica el número de conexiones de red permitidas para su uso por parte de un Agent único para la replicación de los datos de dicha máquina de una vez.

4. Haga clic en **Save (Guardar)**.

Eliminación de replicación

Puede interrumpir la replicación y eliminar las máquinas protegidas de replicación de varias formas. Las opciones incluyen:

- Eliminación de un Agent de la replicación en el Core de origen
- Eliminación de un Agent en el Core de destino
- Eliminación de un Core de destino de la replicación
- Eliminación de un Core de origen de la replicación

NOTA: Eliminar un Core de origen tendrá como resultado la eliminación de todos los Agents replicados protegidos por dicho Core.

Eliminación de un Agent de la replicación en el Core de origen

Para eliminar un Agent de la replicación en el Core de origen:

1. Desde el Core de origen, abra la Core Console y haga clic en la pestaña **Replication (Replicación)**.
2. Expanda la sección **Outgoing Replication (Replicación saliente)**.
3. En el menú desplegable para el Agent que desea eliminar de la replicación, haga clic en **Delete (Eliminar)**.
4. En el cuadro de diálogo **Outgoing Replication (Replicación saliente)**, haga clic en **Yes (Sí)** para confirmar la eliminación.

Eliminación de un Agent en el Core de destino

Para eliminar un Agent en el Core de destino:

1. En el Core de destino, abra la Core Console y haga clic en la pestaña **Replication (Replicación)**.
2. Expanda la sección **Incoming Replication (Replicación entrante)**.
3. En el menú desplegable para el Agent que desee eliminar de la replicación, haga clic en **Delete (Eliminar)** y, a continuación, seleccione una de las opciones siguientes.

Opción	Descripción
Relationship Only (Sólo relación)	Elimina el Agent de la replicación pero mantiene los puntos de recuperación replicados.
With Recovery Point (Con punto de recuperación)	Elimina el Agent de la replicación y elimina todos los puntos de recuperación replicados recibidos de dicha máquina.

Eliminación de un Core de destino de la replicación

Para eliminar un Core de destino de la replicación:

1. En el Core de origen, abra la Core Console y haga clic en la pestaña **Replication (Replicación)**.
2. En **Outgoing Replication (Replicación saliente)**, haga clic en el menú desplegable junto al Core remoto que desee eliminar y haga clic en **Delete (Eliminar)**.
3. En el cuadro de diálogo **Outgoing Replication (Replicación saliente)**, haga clic en **Yes (Sí)** para confirmar la eliminación.

Eliminación de un Core de origen de la replicación

NOTA: Eliminar un Core de origen tendrá como resultado la eliminación de todos los Agents replicados protegidos por dicho Core.

Para eliminar un Core de origen de la replicación:

1. En el Core de destino, abra la Core Console y haga clic en la pestaña **Replication (Replicación)**.
2. Bajo **Incoming Replication (Replicación entrante)**, en el menú desplegable, haga clic en **Delete (Eliminar)** y, a continuación, seleccione una de las opciones siguientes.

Opción	Descripción
Relationship Only (Sólo relación)	Elimina el Core de origen de la replicación pero mantiene los puntos de recuperación replicados.
With Recovery Points (Con puntos de recuperación)	Elimina el Core de origen de la replicación y elimina todos los puntos de recuperación replicados de dicha máquina.

3. En el cuadro de diálogo **Incoming Replication (Replicación entrante)**, haga clic en **Yes (Sí)** para confirmar la eliminación.

Recuperación de datos replicados

La funcionalidad de replicación "Day-to-day" (Día a día) se mantiene en el Core de origen, mientras que solo el Core de destino es capaz de completar las funciones necesarias para la recuperación de desastres.

Para la recuperación de desastres, el Core de destino puede utilizar los puntos de recuperación replicados para recuperar los Agents protegidos y el Core.

Puede realizar las opciones de recuperación siguientes desde el Core de destino:

- Montar puntos de recuperación.
- Revertir a puntos de recuperación.
- Realizar una exportación de máquina virtual (VM).
- Realizar una restauración desce cero (BMR).
- Realizar conmutación por recuperación (en caso de que tenga configurado un entorno de replicación conmutación por error/conmutación por recuperación).

Plan para la conmutación por error y la conmutación por recuperación

Cuando se encuentre con una situación de desastre en la que el Core de origen y el Agent asociado hayan fallado, puede habilitar la conmutación por error en AppAssure para cambiar la protección al Core (destino) de conmutación por error idéntico e iniciar un nuevo Agent (replicado) idéntico al Agent que ha fallado. Después de haber reparado el Core de origen y los Agents, podrá realizar la conmutación por recuperación para restaurar los datos del Core y el Agent con conmutación por error de vuelta al Agent y Core de origen. En AppAssure, la conmutación por error y la conmutación por recuperación implican los siguientes procedimientos.

- Configuración de su entorno para la conmutación por error.
- Realizar una conmutación por error para el Core de destino y el Agent asociado.
- Restaurar un Core de origen realizando la conmutación por recuperación.

Configuración de un entorno para la conmutación por error

Para configurar su entorno para la conmutación por error se requiere tener un Core de origen y de destino y la configuración del Agent asociado para replicación. Complete los pasos que se indican en este procedimiento para configurar la replicación para conmutación por error.

Para configurar un entorno para la conmutación por error:

1. Instale un Core para el origen e instale un Core para el destino.
2. Instale un AppAssure Agent para que lo proteja el Core de origen.
3. Cree un repositorio en el Core de origen y otro en el Core de destino.

   Para obtener más información, consulte Creación de un repositorio.
4. Agregue el Agent para protección en el Core de origen.

   Para obtener más información, consulte Protección de una máquina.
5. Configure la replicación desde el Core de origen al Core de destino y replique el Agent protegido con todos los puntos de recuperación.

   Siga los pasos que se indican en la Replicación a un Core administrado automáticamente para agregar el Core de destino al que va a replicar.

Cómo realizar una conmutación por error en el Core de destino

Cuando encuentre una situación de desastre en la que su Core de origen y Agents asociados han fallado, puede habilitar la conmutación por error para cambiar la protección a su Core de conmutación por error (destino) idéntico. El Core de destino se convierte en el único Core que protege datos en su entorno y, a continuación, inicie un nuevo Agent para reemplazar temporalmente al Agent que ha fallado.

Para realizar una conmutación por error en el Core de destino:

1. Acceda a la Core Console en el Core de destino y haga clic en la ficha **Replication (Replicación)**.
2. En **Incoming Replication (Replicación entrante)**, seleccione el Core de origen y, a continuación, expanda los detalles debajo del Agent individual.
3. En el menú **Actions (Acciones)** para dicho Core, haga clic en **Failover (Conmutación por error)**.

   El estado de esta tabla para esta máquina cambia a **Failover (Conmutación por error)**.
4. Haga clic en la pestaña **Machine (Máquina)** y, a continuación, seleccione la máquina que tenga asociado el Agent AppAssure con puntos de recuperación.
5. Exporte la información del punto de recuperación de copia de seguridad en dicho Agent a una máquina virtual.
6. Apague la máquina que tenga el Agent AppAssure.
7. Inicie la máquina virtual que ahora incluye la información de copia de seguridad exportada.

   Tiene que esperar a que el software del controlador de dispositivos se instale.
8. Reinicie la máquina virtual y espere a que el servicio de Agent se inicie.
9. Vuelva a la Core Console para el Core de destino y compruebe que el Agent nuevo aparece en la pestaña **Machines (Máquinas)** bajo **Protected Machines (Máquinas protegidas)** en la pestaña **Replication (Replicación)** bajo **Incoming Replication (Replicación entrante)**.
10. Fuerce varias instantáneas y compruebe que se completan correctamente.

    Para obtener más información, consulte Cómo forzar una instantánea.
11. Ahora puede continuar realizando la conmutación por recuperación.

    Para obtener más información, consulte Cómo realizar una conmutación por recuperación.

Cómo realizar una conmutación por recuperación

Después de reparar o sustituir el Core de origen que ha fallado y los Agents originales, debe mover los datos desde sus máquinas con conmutación por error para restaurar las máquinas de origen.

Para realizar conmutación por recuperación:

1. Acceda a la Core Console en el Core de destino y haga clic en la ficha **Replication (Replicación)**.
2. En **Incoming Replication (Replicación entrante)**, seleccione el Agent de conmutación por error y expanda los detalles.
3. En el menú **Actions (Acciones)**, haga clic en **Failback (Conmutación por recuperación)**.

   Se abre el cuadro de diálogo **Failback Warnings (Avisos de la Conmutación por recuperación)** para describir los pasos que debe seguir antes de hacer clic en el botón **Start Failback (Iniciar Conmutación por recuperación)**.
4. Haga clic en **Cancel (Cancelar)**.
5. Si la máquina a la que se aplica conmutación por error ejecuta Microsoft SQL Server o Microsoft Exchange Server, detenga estos servicios.
6. En la Core Console para el Core de destino, haga clic en la pestaña **Tools (Herramientas)**.
7. Cree un archivo del Agent de conmutación por error y envíelo como salida a un disco o ubicación de recurso compartido de red.
8. Cuando cree el archivo, acceda a la Core Console en el Core de origen recién reparado, y haga clic en la pestaña **Tools (Herramientas)**.
9. Importe el archivo que acaba de crear en el paso 7.
10. Regrese a la Core Console en el Core de destino y haga clic en la pestaña **Replication (Replicación)**.
11. En **Incoming Replication (Replicación entrante)**, seleccione el Agent de conmutación por error y expanda los detalles.
12. En el menú **Actions (Acciones)**, haga clic en **Failback (Conmutación por recuperación)**.
13. En el cuadro de diálogo **Failback Warnings (Avisos de conmutación por recuperación)**, haga clic en **Start Failback (Iniciar conmutación por recuperación)**.
14. Apague la máquina que tiene el Agent exportado que se ha creado durante la conmutación por error.
15. Realice una restauración desde cero (BMR) para el Core de origen y el Agent.

    NOTA: Cuando inicie la restauración, deberá usar los puntos de recuperación que se importaron desde el Core de origen hasta el Agent en la máquina virtual.
16. Espere a que se vuelva a iniciar la BMR y que se reinicie el servicio de Agent y, a continuación, revise y registre los detalles de conexión de red de la máquina.
17. Acceda a la Core Console en el Core de origen y, en la pestaña **Machines (Máquinas)**, modifique las configuraciones de protección de máquina para agregar los detalles de la conexión de red nueva.
18. Vaya a la Core Console en el Core de destino y elimine el Agent de la pestaña **Replication (Replicación)**.
19. En la Core Console del Core de origen, vuelva a configurar la replicación entre el origen y el destino haciendo clic en la pestaña **Replication (Replicación)** y, a continuación, agregue el Core de destino para replicación.

Administración de eventos

La administración de eventos de Core ayuda en la supervisión del estado y el uso de Core. El Core incluye conjuntos de eventos predefinidos, que se pueden utilizar para notificar a los administradores de problemas críticos del Core o los trabajos de copia de seguridad.

En la pestaña **Events (Eventos)**, puede administrar grupos de notificación, la configuración SMTP de correo electrónico, la reducción de repeticiones y la retención de eventos. La opción Notification Groups (Grupos de notificación) le permite administrar grupos de notificación, desde los que podrá:

- Especificar un evento para el cual desee generar una alerta en los casos siguientes:

  - Clusters
  - Attachability
  - Trabajos
  - Licencias
  - Log Truncation (Truncamiento de registro)
  - Archive
  - Core Service (Servicio de Core)
  - Exportar
  - Protection
  - Replicación
  - Rollback
  - Configuración del servidor SMTP
  - Registros de seguimiento habilitados
  - Configuración de servicios en la nube
- Especificar el tipo de alerta (error, aviso o informativa).
- Especificar a quién y dónde se envían las alertas. Las opciones incluyen:
  - Dirección de correo electrónico
  - Registros de eventos de Windows
  - Servidor Syslog
- Especificar un umbral de tiempo para la repetición.
- Especificar el período de retención de todos los eventos.

Configuración de grupos de notificación

Para configurar grupos de notificación:

1. En Core, seleccione la pestaña **Configuration (Configuración)**.
2. En la opción **Manage (Administrar)**, haga clic en **Events (Eventos)**.
3. Haga clic en **Add Group (Agregar grupo)**.

   Aparece el cuadro de diálogo **Add Notification Group (Agregar grupo de notificación)** y muestra tres paneles:
   - **General**
   - **Enable Events (Habilitar eventos)**
   - **Notification Options (Opciones de notificación)**
4. En el panel **General**, introduzca información básica para el grupo de notificación, como se describe a continuación:

Cuadro de texto	Descripción
Nombre	Introduzca un nombre para el grupo de notificación de eventos. Se utiliza para identificar el grupo de notificación de eventos.
Descripción	Introduzca una descripción para el grupo de notificación de eventos. Se utiliza para describir el propósito del grupo de notificación de eventos.

5. En el panel **Enable Events (Habilitar eventos)**, seleccione las condiciones por las que se crearán registros de eventos (alertas) y se informará de ellos.

   Puede decidir crear alertas para:

- **All Events (Todos los eventos)**
- **Appliance Events (Eventos de servidor)**
- **Boot CD (CD de inicio)**
- **Seguridad**
- **DatabaseRetention**
- **LocalMount**
- **Clusters**
- **Notification (Notificación)**
- **Power Shell Scripting (Secuencias de comandos de Power Shell)**
- **Push Install (Instalación de inserción)**
- **Nightly Jobs (Trabajos nocturnos)**
- **Attachability**
- **Trabajos**
- **Licencias**
- **Log Truncation (Truncamiento de registro)**
- **Archive**
- **Core Service (Servicio de Core)**
- **Exportar**
- **Protection**
- **Replicación**
- **Repository (Repositorio)**
- **Rollback**
- **Rollup**

6. En el panel **Notification Options (Opciones de notificación)**, especifique cómo se tramitará el proceso de notificación.

   Las opciones de notificación son:

Cuadro de texto	Descripción
Notify by e-mail (Notificar por correo electrónico)	Designe los destinatarios de la notificación por correo electrónico. Puede elegir especificar varias direcciones de correo electrónico individuales, así como copias ocultas. Puede elegir: • **A:** • **CC:** • **CCO:**
Notify by Windows Event Log (Notificar mediante registro de eventos de Windows)	Seleccione esta opción si desea informar de las alertas a través del registro de eventos de Windows. Se utiliza para especificar si la notificación de alertas debe comunicarse a través del registro de eventos de Windows.
Notify by sys logd (Notificar por sys logd)	Seleccione esta opción si desea informar de las alertas a través de sys logd. Especifique los detalles para el sys logd en los siguientes cuadros de texto: • **Nombre del host:**

Cuadro de texto	Descripción
	• **Puerto: 1**

7. Haga clic en **OK (Aceptar)**.

Configuración de un servidor de correo electrónico y de una plantilla de notificaciones de correo electrónico

Si desea recibir notificaciones de correo electrónico acerca de eventos, configure un servidor de correo electrónico y una plantilla de notificaciones de correo electrónico.

NOTA: También deberá configurar los valores del grupo de notificación, además de activar la opción **Notify by email (Notificar por correo electrónico)**, antes de que se envíen los mensajes de alerta por correo electrónico. Para obtener más información acerca de cómo especificar eventos para recibir alertas por correo electrónico, consulte Configuring Notification Groups For System Events (Configuración de grupos de notificación para eventos del sistema).

Para configurar un servidor de correo electrónico y una plantilla de notificaciones de correo electrónico:

1. En Core, seleccione la pestaña **Configuration (Configuración)**.
2. En la opción **Manage (Administrar)**, haga clic en **Events (Eventos)**.
3. En el panel **Email SMTP Settings (Configuración SMTP de correo electrónico)**, haga clic en **Change (Cambiar)**.

   Aparecerá el cuadro de diálogo Edit **Email Notification Configuration (Editar configuración de notificación por correo electrónico)**.
4. Seleccione **Enable Email Notifications (Habilitar notificaciones de correo electrónico)** y, a continuación, introduzca los detalles para el servidor de correo electrónico de la siguiente manera:

Cuadro de texto	Descripción
SMTP Server	Introduzca el nombre del servidor de correo electrónico que utilizará la plantilla de notificaciones de correo electrónico. La convención de nombres incluye el nombre de host, el dominio y el sufijo; por ejemplo, **smtp.gmail.com**.
Port	Introduzca un número de puerto. Se utiliza para identificar el puerto para el servidor de correo electrónico. Por ejemplo, el puerto 587 para Gmail. El valor predeterminado es 25.
Timeout (seconds)	Introduzca un valor entero para especificar cuánto tiempo debe intentar una conexión antes de que se agote el tiempo de espera. Se utiliza para establecer el tiempo, en segundos, durante el que se intenta la conexión al servidor de correo electrónico antes de que se agote el tiempo de espera. El valor predeterminado es 30 segundos.
TLS	Seleccione esta opción si el servidor de correo electrónico utiliza una conexión segura como, por ejemplo, Seguridad de la capa de transporte (TLS) o Capa de sockets seguros (SSL).
Nombre de usuario	Introduzca un nombre de usuario para el servidor de correo electrónico.

Cuadro de texto	Descripción
Contraseña	Introduzca una contraseña para acceder al servidor de correo electrónico.
From	Introduzca una dirección de correo electrónico del remitente. Se utiliza para especificar la dirección de correo electrónico del remitente para la plantilla de notificaciones de correo electrónico; por ejemplo, **noreply@localhost.com**.
Email Subject	Introduzca un asunto para la plantilla de correo electrónico. Se utiliza para definir el asunto de la plantilla de notificaciones de correo electrónico; por ejemplo, `<hostname> - <level> <name>`.
Email	Introduzca la información para el texto de la plantilla que describe el evento, cuándo se ha producido y la gravedad.

5. Haga clic en **Send Test Email (Enviar correo electrónico de prueba)** y revise los resultados.
6. Cuando los resultados de la prueba sean satisfactorios, haga clic en **OK (Aceptar)**.

Configuración de la reducción de repeticiones

Para configurar la reducción de repeticiones:

1. En el Core, haga clic en la pestaña **Configuration (Configuración)**.
2. En la opción **Manage (Administrar)**, haga clic en **Events (Eventos)**.
3. En el área **Repetition Reduction (Reducción de repeticiones)**, haga clic en **Change (Cambiar)**.
   Aparecerá el cuadro de diálogo Repetition Reduction (Reducción de repeticiones).
4. Seleccione **Enable Repetition Reduction (Habilitar reducción de repeticiones)**.
5. En el cuadro de texto **Store events for X minutes (Almacenar eventos durante X minutos)**, introduzca el número de minutos durante los que se almacenarán los eventos para la reducción de repeticiones.
6. Haga clic en **OK (Aceptar)**.

Configuración de la retención de eventos

Para configurar la retención de eventos:

1. En el Core, haga clic en la pestaña **Configuration (Configuración)**.
2. En la opción **Manage (Administrar)**, haga clic en **Events (Eventos)**.
3. En **Database Connection Settings (Configuración de conexión de base de datos)**, haga clic en **change (cambiar)**.
   Aparecerá el cuadro de diálogo **Database Connection Settings (Configuración de conexión de base de datos)**.
4. En el cuadro de texto **Retain event and job history for (Conservar historial de sucesos y trabajos durante)**, introduzca el número de días que desea conservar la información sobre los eventos.
   Por ejemplo, puede seleccionar 30 días (predeterminado).
5. Haga clic en **Save (Guardar)**.

Administración de la recuperación

Core puede restaurar datos o recuperar máquinas en máquinas físicas o virtuales instantáneamente desde los puntos de recuperación. Los puntos de recuperación contienen instantáneas de volúmenes de Agents capturadas a nivel de bloque. Estas instantáneas son sensibles a las aplicaciones, lo que implica

que se completen todas las transacciones abiertas y registros de transacciones en movimiento y que las cachés se despejen a disco antes de crear la instantánea. El uso de instantáneas sensibles a las aplicaciones junto con Verified Recovery (Recuperación verificada) permite al Core realizar varios tipos de recuperaciones, que incluyen:

- Recuperación de archivos y carpetas
- Recuperación de volúmenes de datos, mediante Live Recovery
- Recuperación de volúmenes de datos para Microsoft Exchange Server y Microsoft SQL Server, mediante Live Recovery
- Restauración desde cero, mediante Universal Recovery
- Recuperación desde cero de hardware diferente, mediante Universal Recovery
- Exportación ad-hoc y continua a máquinas virtuales

Acerca de la información del sistema

AppAssure le permite ver información sobre Core, que incluye información del sistema, volúmenes locales y montados y conexiones del motor de AppAssure.

Si quiere desmontar puntos de recuperación individuales (o incluso todos) que estén montados localmente en un Core, puede hacerlo desde la opción **Mount (Montar)** en la pestaña **Tools (Herramientas)**.

Visualización de la información del sistema

Para ver la información del sistema:

1. Vaya al Core y seleccione la pestaña **Tools (Herramientas)**.
2. En la opción **Tools (Herramientas)**, haga clic en **System Info (Información del sistema)**.

Descarga de instaladores

Puede descargar instaladores desde el Core. En la pestaña **Tools (Herramientas)**, puede elegir descargar el instalador Agent o la Local Mount Utility (Utilidad de montaje local).

NOTA: Para acceder al instalador Agent, consulte Descarga e instalación del instalador Agent. Para obtener más información sobre la implementación del instalador Agent, consulte la *Dell DL4000 Appliance Deployment Guide (Guía de implementación del appliance Dell DL4000)* en **dell.com/support/home**. Para acceder al Local Mount Utility Installer (Instalador de la Utilidad de montaje local), consulte Acerca de la Utilidad de montaje local, y para obtener más información sobre la Local Mount Utility (Utilidad de montaje local), consulte Descarga e instalación de la Local Mount Utility (Utilidad de montaje local).

Acerca del instalador Agent

El instalador Agent se utiliza para instalar la aplicación AppAssure Agent en máquinas concebidas para ser protegidas mediante Core. Si determina que dispone de una máquina que necesita el instalador Agent, puede descargar el instalador web desde la pestaña **Tools (Herramientas)** en el Core.

NOTA: La descarga del Core se realiza desde el Portal de licencias. Para descargar el instalador del Core, visite **https://licenseportal.com**.

Descarga e instalación del instalador Agent

Puede descargar e implementar el instalador Agent en cualquier máquina protegida por el Core.

Para descargar e instalar el instalador Agent:

1. Descargue el instalador Agent desde el Portal de Licencias o desde el Core.

   Por ejemplo: Agent-X64-5.3.x.xxxxx.exe
2. Haga clic en **Save File (Guardar archivo)**.

   Para obtener más información sobre cómo instalar los Agents, consulte la *Dell DL4000 Appliance Deployment Guide (Guía de implementación del appliance Dell DL4000)* en **dell.com/support/home**.

Acerca de la Utilidad de montaje local

La Local Mount Utility (Utilidad de montaje local - LMU) es una aplicación descargable que le permite montar un punto de recuperación en un Core remoto desde cualquier máquina. La utilidad ligera incluye los controladores `aavdisk` y `aavstor`, aunque no se ejecuta como un servicio. La utilidad se instala de manera predeterminada en el directorio C:\Program Files\AppRecovery\Local Mount Utility y se muestra un acceso directo en el escritorio de la máquina.

Aunque la utilidad se diseñó para el acceso remoto a Cores, también puede instalar la LMU en el Core. Cuando se ejecuta en un Core, la aplicación reconoce y muestra todos los montajes desde ese Core, incluidos los montajes realizados mediante la Core Console. Asimismo, también se muestran los montajes realizados en la LMU en la consola.

Descarga e instalación de la Local Mount Utility (Utilidad de montaje local)

Para descargar e instalar la Local Mount Utility (Utilidad de montaje local):

1. En la máquina en la que desea instalar la LMU, acceda a la Core Console introduciendo la URL de la consola en su navegador e iniciando sesión con su nombre de usuario y contraseña.
2. En la Core Console, haga clic en la pestaña **Tools (Herramientas)**.
3. En la pestaña **Tools (Herramientas)**, haga clic en **Downloads (Descargas)**.
4. En la **Local Mount Utility (Utilidad de montaje local)**, haga clic en el enlace **Download web installer (Descargar instalador web)**.
5. En la ventana **Opening LocalMountUtility-Web.exe (Abrir LocalMountUtility-Web.exe)**, haga clic en **Save File (Guardar archivo)**.

   El archivo se guarda en la carpeta Downloads (Descargas) local. En algunos exploradores, la carpeta se abre automáticamente.
6. En la carpeta **Downloads (Descargas)**, haga clic con el botón derecho del mouse sobre el ejecutable **LocalMountUtility-Web** y haga clic en **Open (Abrir)**.

   Dependiendo de la configuración de su máquina, puede que aparezca la ventana **User Account Control (Control de cuenta de usuario)**.
7. Si aparece la ventana **User Account Control (Control de cuenta de usuario)**, haga clic en **Yes (Sí)** para permitir al programa realizar los cambios en la máquina.

   Se inicia el asistente **AppAssure Local Mount Utility Installation (Instalación de la utilidad de montaje local de AppAssure)**.

8. En la pantalla **Welcome (Bienvenida)** del asistente de **AppAssure Local Mount Utility Installation (Instalación de la utilidad de montaje local de AppAssure)**, haga clic en **Next (Siguiente)** para pasar a la página **License Agreement (Contrato de licencia)**.
9. En la pantalla **License Agreement (Contrato de licencia)**, seleccione **I accept the terms in the license agreement (Acepto las condiciones del contrato de licencia)** y, a continuación, haga clic en **Next (Siguiente)** para pasar a la página **Prerequisites (Requisitos previos)**.
10. En la página **Prerequisites (Requisitos previos)**, instale los requisitos previos necesarios, y haga clic en **Next (Siguiente)** para continuar a la página **Installation Options (Opciones de instalación)**.
11. En la página **Installation Options (Opciones de instalación)**, realice las tareas siguientes:
    a. Elija una carpeta de destino para la LMU haciendo clic en el botón **Change (Cambiar)**.

       NOTA: La carpeta de destino predeterminada es C:\Program Files\AppRecovery \LocalMountUtility.
    b. Seleccione si quiere o no **Allow Local Mount Utility to automatically send diagnostic and usage information to AppAssure Software, Inc. (Permitir que Local Mount Utility envíe automáticamente información de uso y diagnóstico a AppAssure Software, Inc.)**.
    c. Haga clic en **Next (Siguiente)** para ir a la página **Progress (Progreso)** y descargar la aplicación. La aplicación se descarga en la carpeta de destino, con el progreso mostrado en la barra de progreso. Cuando haya terminado, el asistente se dirigirá automáticamente a la página **Completed (Completado)**.
12. Haga clic en **Finish (Terminar)** para cerrar el asistente.

Cómo agregar un Core a la Local Mount Utility (Utilidad de montaje local)

Para montar un punto de recuperación, debe agregar el Core a LMU. No hay límite respecto al número de Cores que puede agregar.

Para agregar un Core a la Local Mount Utility (Utilidad de montaje local):

1. En la máquina en la que esté instalada la utilidad LMU, iníciela haciendo doble clic en el icono del escritorio.
2. Si aparece la ventana **User Account Control (Control de cuenta de usuario)**, haga clic en **Yes (Sí)** para permitir al programa realizar los cambios en la máquina.
3. En la esquina superior izquierda de la ventana Local Mount Utility (Utilidad de montaje local) de AppAssure, haga clic en **Add core (Agregar Core).**
4. En la ventana **Add Core (Agregar Core)**, introduzca las credenciales necesarias, tal como se describe a continuación:

Cuadro de texto	Descripción
Host Name (Nombre del host)	El nombre del Core desde el que desee montar puntos de recuperación. NOTA: Si instala la LMU en un Core, la LMU agrega automáticamente la máquina de host local.
Port	Número de puerto usado para comunicarse con el Core. El número de puerto predeterminado es 8006.
Use my Windows user credentials (Utilizar mis credenciales de	Seleccione esta opción si las credenciales que utiliza para acceder al Core son las mismas que sus credenciales de Windows.

Cuadro de texto	Descripción
usuario de Windows)	
Use specific credentials (Utilizar credenciales específicas)	Seleccione esta opción si las credenciales que utiliza para acceder al Core son distintas de las credenciales de Windows.
Nombre de usuario	Nombre de usuario utilizado para acceder a la máquina del Core. NOTA: Esta opción sólo está disponible si elije usar credenciales específicas.
Contraseña	Contraseña utilizada para acceder a la máquina del Core. NOTA: Esta opción sólo está disponible si elije usar credenciales específicas.

5. Haga clic en **Connect (Conectar)**.
6. Si agrega varios Cores, repita los pasos que van del 3 al 5 según sea necesario.

Montaje de un punto de recuperación mediante la Local Mount Utility (Utilidad de montaje local)

Antes de montar un punto de recuperación, la LMU debe conectarse con el Core en el que se almacena el punto de recuperación. Como se describe en Agregar un core a la Utilidad de montaje local, el número de Cores que pueden agregarse a la LMU es ilimitado; sin embargo, la aplicación solo puede conectarse a un Core a la vez. Por ejemplo, si monta un punto de recuperación de un Agent protegido por un Core y, a continuación, monta un punto de recuperación de un Agent protegido por un Core diferente, la LMU se desconecta automáticamente del primer Core para establecer una conexión con el segundo Core.

Para montar un punto de recuperación mediante la Local Mount Utility (Utilidad de montaje local):

1. En la máquina en la que esté instalada la utilidad LMU, iníciela haciendo doble clic en el icono del escritorio.
2. En la ventana principal de **Local Mount Utility de AppAssure (Utilidad de montaje local de Appassure)**, expanda el Core que quiera en el árbol de navegación para mostrar los Agents protegidos.
3. Seleccione el Agent deseado desde el árbol de navegación.

   Los puntos de recuperación se muestran en el marco principal.
4. Expanda el punto de recuperación que desee montar para revelar volúmenes de disco o bases de datos individuales.
5. Haga clic con el botón derecho del mouse en el punto de recuperación que desee montar y seleccione una de las siguientes opciones:
   - Mount (Montar)
   - Mount Writable (Montaje con capacidad de escritura)
   - Mount with previous writes (Montar con escrituras anteriores)
   - Advanced mount (Montaje avanzado)
6. En la ventana **Advanced Mount (Montaje avanzado)**, complete las opciones que se describen a continuación:

Cuadro de texto	Descripción
Mount point path (Ruta de acceso de punto de montaje)	Para seleccionar una ruta de acceso para los puntos de recuperación distinta de la ruta de acceso del punto de montaje predeterminado, haga clic en el botón **Browse (Examinar)**.
Mount Type (Tipo de montaje)	Seleccione una de las opciones siguientes: • Mount Read-only (Montaje de solo lectura) • Mount Writable (Montaje con capacidad de escritura) • Mount Read-only with previous writes (Montaje de solo lectura con escrituras anteriores)

7. Haga clic en **Mount (Montar)**.

La LMU abre automáticamente la carpeta que contiene el punto de recuperación montado.

NOTA: Si selecciona un punto de recuperación que ya está montado, se abrirá el diálogo **Mounting (Montaje)** para solicitarle que desmonte el punto de recuperación.

Exploración de un punto de recuperación montado mediante la Local Mount Utility (Utilidad de montaje local)

NOTA: Este procedimiento no es necesario si está explorando un punto de recuperación justo después de montarlo, ya que la carpeta que contiene el punto de recuperación se actualiza automáticamente al completar el procedimiento de montaje.

Para explorar un punto de recuperación montado mediante la Local Mount Utility (Utilidad de montaje local):

1. En la máquina en la que esté instalada la LMU, iníciela haciendo doble clic en el icono del escritorio.
2. En la pantalla principal de **Local Mount Recovery (Recuperación de montaje local)**, haga clic en **Active mounts (Montajes activos)**.

   Se abre la ventana **Active Mounts (Montajes activos)** y muestra todos los puntos de recuperación montados.
3. Haga clic en **Explore (Explorar)** junto al punto de recuperación para abrir la carpeta de volúmenes desduplicados.

Desmontaje de un punto de recuperación mediante la Local Mount Utility (Utilidad de montaje local)

Para demostrar un punto de recuperación utilizando la Local Mount Utility (Utilidad de montaje local)

1. En la máquina en la que esté instalada la utilidad LMU, iníciela haciendo doble clic en el icono del escritorio.
2. En la pantalla principal de **Local Mount Recovery (Recuperación de montaje local)**, haga clic en **Active mounts (Montajes activos)**.

   Se abre la ventana **Active Mounts (Montajes activos)** y muestra todos los puntos de recuperación montados.
3. Seleccione una de las opciones descritas en la tabla siguiente para desmontar puntos de recuperación.

Opción	Descripción
Dismount (Desmontar)	Desmonta solo el punto de recuperación adyacente. a. Haga clic en **Dismount (Desmontar)** junto al punto de recuperación en cuestión. b. Cierre la ventana.
Dismount all (Desmontar todo)	Desmonta todos los puntos de recuperación montados. a. Haga clic en **Dismount all (Desmontar todo)**. b. En la ventana **Dismount All (Desmontar todo)**, haga clic en **Yes (Sí)** para confirmar. c. Cierre la ventana.

Acerca del menú de bandeja de la Local Mount Utility (Utilidad de montaje local)

El menú de bandeja de la LMU se encuentra en la barra de tareas del escritorio. Haga clic con el botón derecho del mouse en el icono para que aparezcan las siguientes opciones:

Browse Recovery Points (Examinar puntos de recuperación)	Abre la pantalla principal de LMU.
Active Mounts (Montajes activos).	Abre la pantalla Active Mounts (Montajes activos).
Opciones	Abre la pantalla Options (Opciones), en la que puede cambiar el **Default Mount Point Directory (Directorio predeterminado de punto de montaje)**, las **Default Core Credentials (Credenciales predeterminadas de Core)** y el **Language (Idioma)** para la interfaz de usuario de LMU.
About (Acerca de)	Abre la pantalla emergente con la información de licencia.
Exit (Salir)	Cierra la aplicación.

NOTA: Con la X en la esquina superior de la pantalla principal se minimiza la aplicación a la bandeja.

Uso de las opciones de Core y Agent

Al hacer clic con el botón derecho del mouse sobre la pantalla principal de la LMU, podrá usar ciertas opciones:

- Opciones de Localhost (Host local)
- Opciones de Remote Core (Core remoto)
- Opciones de Agent

Acceso a las opciones del localhost

Para acceder a las opciones de Localhost, haga clic con el botón derecho del mouse en Core o en Agent y, a continuación, haga clic en **Reconnect (Volver a conectarse)** al Core. La información del Core se actualiza y renueva; por ejemplo, Agents agregados recientemente.

Acceso a las opciones del Core remoto

Para acceder a las opciones del Core remoto, haga clic con el botón derecho del mouse en Core o Agent y, a continuación, seleccione una de las opciones del Core remoto, según se describe a continuación:

Opción	Descripción
Reconnect to core (Volver a conectar con el Core)	Renueva y actualiza la información desde el Core, como Agents agregados recientemente.
Remove core (Eliminar Core)	Elimina el Core de la **Local Mount Utility (Utilidad de montaje local)**.
Edit core (Editar Core)	Abre la ventana **Edit Core (Editar Core)**, en la que puede cambiar el nombre de host, puerto y credenciales.

Acceso a opciones de Agent

Para acceder a las opciones de Agent, haga clic con el botón derecho del mouse en el Core o en el Agent y, a continuación, haga clic en **Refresh recovery points (Renovar puntos de recuperación)**. Se actualizará la lista de puntos de recuperación del Agent seleccionado.

Administración de políticas de retención

Las instantáneas de copia de seguridad periódicas de todos los servidores protegidos se van acumulando en el Core con el paso del tiempo. Las políticas de retención sirven para conservar instantáneas de copia de seguridad durante más tiempo y para optimizar la administración de las mismas. Además, estas políticas se aplican mediante un proceso de mantenimiento nocturno que permite determinar la antigüedad y eliminar las copias de seguridad antiguas. Para obtener más información acerca de cómo configurar políticas de retención, consulte Personalización de la configuración de las políticas de retención.

Archivado en una nube

Para archivar los datos en una nube puede transferirlos a una variedad de proveedores de servicios en la nube directamente desde la Core Console. Las nubes compatibles incluyen Windows Azure, Amazon, Rackspace y cualquier proveedor basado en el estándar OpenStack.

Para exportar un archivo a una nube:

- Agregue su cuenta de servicios en la nube a la Core Console. Para obtener más información, consulte Cómo agregar una cuenta de servicios en la nube.
- Archive los datos y exportélos a su cuenta de nube.
- Recupere los datos archivados importando desde la ubicación en la nube.

Acerca del archivado

Las políticas de retención establecen los períodos durante los cuales las copias de seguridad se almacenan en medios a corto plazo (rápidos y caros). A veces, determinados requisitos empresariales y técnicos exigen ampliar la retención de estas copias de seguridad, pero el uso de almacenamiento rápido resulta inasequible. Por tanto, este requisito crea una necesidad de almacenamiento a largo plazo (lento y barato). Las empresas a menudo utilizan el almacenamiento a largo plazo para archivar datos de cumplimiento y de no cumplimiento. La función de archivo en AppAssure se utiliza para admitir la retención ampliada de datos de cumplimiento y de no cumplimiento. También se utiliza para inicializar los datos de replicación en un Core de réplica remoto.

Creación de un archivo

Para crear un archivo

1. En la Core Console, haga clic en la pestaña **Configuration (Configuración)**.
2. En la opción **Manage (Administrar)**, haga clic en **Archive (Archivo)**.
   Aparecerá el cuadro de diálogo **Create Archive (Crear archivo)**.
3. En el cuadro de diálogo **Create Archive (Crear archivo)**, introduzca los detalles del archivo tal como se describe a continuación:

Cuadro de texto	Descripción
Date range (Intervalo de fechas)	Para especificar el intervalo de fechas, seleccione las fechas de inicio y de finalización.
Archive password (Contraseña de archivo)	Introduzca una contraseña para el archivo. Se utiliza para establecer las credenciales de inicio de sesión que protegen el archivo.
Confirm (Confirmar)	Vuelva a introducir la contraseña para proteger el archivo. Se utiliza para proporcionar una validación de la información que introdujo en el cuadro de texto **Archive Password (Contraseña de archivo)**.
Output Location (Ubicación de salida)	Introduzca la ubicación de la salida. Se utiliza para definir la ruta de acceso de ubicación en la que desea que resida el archivo. Puede ser un disco local o un recurso compartido de red. Por ejemplo, **d:\work\archive** o **\\servername \sharename** para las rutas de acceso de red. **NOTA:** Si la ubicación de salida es un recurso compartido de red, introduzca un nombre de usuario y una contraseña para conectar con el recurso compartido.
Nombre de usuario	Introduzca un nombre de usuario. Se utiliza para establecer las credenciales de inicio de sesión para el recurso compartido de red.
Contraseña	Introduzca una contraseña para la ruta de acceso de red. Se utiliza para establecer las credenciales de inicio de sesión para el recurso compartido de red.

Cuadro de texto	Descripción
Tamaño máximo	Introduzca la cantidad de espacio que utilizará para el archivo. Puede seleccionar entre: • Destino completo • Una cantidad específica en MB o GB
Recycle action (Acción de reciclaje)	Seleccione la acción de reciclaje adecuada.
Comment	Introduzca la información adicional que sea necesaria capturar para el archivo.

4. Haga clic en **Archive (Archivo)**.

Configuración del archivado programado

La función Scheduled Archive (Archivado programado) le permite establecer la hora en la que se creará un archivado de una máquina seleccionada y se guardará en la ubicación especificada. Esta función se adaptará a ese tipo de situaciones en las que tendrá que elegir el lugar donde guardar archivados frecuentes de una máquina, sin la incomodidad de tener que crearlos manualmente. Complete los pasos del siguiente procedimiento para programar archivados automáticos.
Para establecer archivados programados:

1. En la Core Console, haga clic en la pestaña **Tools (Herramientas)**.
2. En la opción de **Archive (Archivado)**, haga clic en **Scheduled (Programado)**.
3. En la página Scheduled Archive (Archivado programado), haga clic en **Add (Agregar**).
   Aparecerá el cuadro de diálogo del asistente **Add Archive Wizard (Asistente para agregar archivado)**.
4. En la página **Location (Ubicación)** del **Add Archive Wizard (Asistente para agregar archivo)**, seleccione una de las opciones siguientes en la lista desplegable **Location Type (Tipo de ubicación)**:
   - Local: ubicación de salida: introduzca la ubicación de la salida. Define la ruta de acceso de ubicación en la que desea que resida el archivado.
   - Network (Red)
     - Output location (Ubicación de salida): introduzca la ubicación de la salida. Define la ruta de acceso de ubicación en la que desea que resida el archivado.
     - User Name (Nombre de usuario): introduzca un nombre de usuario. Se establecen las credenciales de inicio de sesión para el recurso compartido de red.
     - Password (Contraseña): introduzca una contraseña para la ruta de acceso de red. Se establecen las credenciales de inicio de sesión para el recurso compartido de red.
   - Cloud (Nube)
     - Account (Cuenta): seleccione una cuenta desde la lista desplegable. Para seleccionar una cuenta de servicios en la nube, debe haberla agregado primero en la Core Console.
     - Container (Contenedor): en el menú desplegable, seleccione un contenedor asociado con la cuenta.
     - Folder Name (Nombre de la carpeta): escriba un nombre para la carpeta en la que se van a guardar los datos archivados. El nombre predeterminado es AppAssure-5-Archive-[FECHA DE CREACIÓN]-[HORA DE CREACIÓN]
5. Haga clic en **Next (Siguiente)**.
6. En la página **Machines (Máquinas)** del asistente, seleccione las máquinas protegidas que contienen los puntos de recuperación que desea archivar.

7. Haga clic en **Next (Siguiente)**.
8. En la página **Options (Opciones)**, seleccione una de las siguientes Acciones de reciclaje de la lista desplegable:
   - **Replace this Core (Reemplazar este Core)**:sobrescribe los datos archivados que ya existen y que pertenecen a este Core, pero deja intactos los datos de los otros Cores.
   - **Erase completely (Borrar completamente)**: borra todos los datos archivados del directorio antes de escribir el archivo nuevo.
   - **Incremental (Incremental)**: permite agregar puntos de recuperación a un archivo existente. Compara los puntos de recuperación para evitar duplicar datos que ya existen en el archivo.
9. En la página **Schedule (Programa)**, seleccione una de las siguientes opciones de frecuencia de envío de datos:
   - Daily (Diariamente): At time (A las): seleccione la hora del día en la que desea crear un archivado diario.
   - Semanalmente
     - At day of week (En el día de la semana): seleccione un día de la semana en el que desea crear el archivado automáticamente.
     - At time (A las): seleccione la hora del día en la que desea crear un archivado diario.
   - Mensualmente
     - At day of months (En el día del mes): seleccione el día del mes en el que desea crear el archivado automáticamente.
     - At time (A las): seleccione la hora del día en la que desea crear un archivado diario.
10. Para pausar el archivado y reanudarlo más tarde, seleccione **Initial pause archiving (Pausa inicial del archivado).**

    Es posible que desee pausar el archivado programado si necesita tiempo para preparar la ubicación de destino antes de archivar reanudaciones. Si no se selecciona esta opción, el archivado comienza a la hora programada.
11. Haga clic en **Finish (Finalizar)**.

Pausa o Reanudación de un archivado programado

Si ha optado por pausar inicialmente el archivado cuando realice el procedimiento de archivado programado, es probable que desee reanudar el archivado programado en otro momento.
Para hacer una pausa o reanudar el archivado programado:

1. Vaya a la **Core Console** y seleccione la pestaña **Tools (Herramientas)**.
2. En la opción **Archive (Archivado)**, haga clic en **Scheduled (Programado)**.
3. En la página **Scheduled Archive (Archivado programado)**, realice una de las acciones siguientes:
   - Seleccione el archivo que prefiera y, a continuación, haga clic en una de las siguientes acciones, según corresponda:
     - Pause (Pausa)
     - Resume (Reanudar)
   - Junto al archivado preferido, haga clic en el menú desplegable y, a continuación, haga clic en una de las siguientes acciones, según corresponda:
     - Pause (Pausa)
     - Resume (Reanudar)

   El estado del archivado se muestra en la columna **Schedule (Programa)**.

Edición de un archivado programado

1. En la Core Console, haga clic en la pestaña **Tools (Herramientas)**.
2. En la opción de **Archive (Archivado)** , haga clic en **Scheduled (Programado)**.
3. En la página Scheduled Archive (Archivado programado), haga clic en el menú desplegable junto a los archivos que desea cambiar y, a continuación, haga clic en **Edit (Editar)**.

   Aparecerá el cuadro de diálogo **Add Archive Wizard (Asistente para agregar archivado)**.
4. En la página **Create (Crear)** del **Add Archive Wizard (Asistente para agregar archivado)**, seleccione una de las opciones siguientes en la lista desplegable **Location Type (Tipo de ubicación)**:
   - Local: Output location (Local: ubicación de salida): introduzca la ubicación de la salida. Se define la ruta de acceso de ubicación en la que desea que resida el archivo.
   - Network (Red)
     - Output location (Ubicación de salida): introduzca la ubicación de la salida. Se define la ruta de acceso de ubicación en la que desea que resida el archivo.
     - User Name (Nombre de usuario): introduzca un nombre de usuario. Se establecen las credenciales de inicio de sesión para el recurso compartido de red.
     - Password (Contraseña): introduzca una contraseña para la ruta de acceso de red. Se establecen las credenciales de inicio de sesión para el recurso compartido de red.
   - Cloud (Nube)
     - Account (Cuenta): seleccione una cuenta desde la lista desplegable. Para seleccionar una cuenta de servicios en la nube, debe haberla agregado primero en la Core Console.
     - Container (Contenedor): en el menú desplegable, seleccione un contenedor asociado a la cuenta.
     - Folder Name (Nombre de la carpeta): escriba un nombre para la carpeta en la que se van a guardar los datos archivados. El nombre predeterminado es AppAssure-5-Archive-[FECHA DE CREACIÓN]-[HORA DE CREACIÓN]
5. Haga clic en **Next (Siguiente)**.
6. En la página **Machines (Máquinas)** del asistente, seleccione las máquinas protegidas que contienen los puntos de recuperación que desea archivar.
7. Haga clic en **Next (Siguiente)**.
8. En la página **Schedule (Programa)**, seleccione una de las siguientes opciones de frecuencia de envío de datos:
   - Daily (Diariamente): At time (A las): seleccione la hora del día en la que desea crear un archivado diario.
   - Semanalmente
     - At day of week (En el día de la semana): seleccione un día de la semana en el que desea crear el archivado automáticamente.
     - At time (A las): seleccione la hora del día en la que desea crear un archivado diario.
   - Mensualmente
     - At day of months (En el día del mes): seleccione el día del mes en el que desea crear automáticamente el archivado.
     - At time (A las): seleccione la hora del día en la que desea crear un archivado diario.
9. Para pausar el archivado y reanudarlo más tarde, seleccione **Initial pause archiving (Pausa inicial del archivado).**

Es posible que desee pausar el archivado programado si necesita tiempo para preparar la ubicación de destino antes de archivar reanudaciones. Si no se selecciona esta opción, el archivado comienza a la hora programada.

10. Haga clic en **Finish (Finalizar)**.

Comprobación de un archivo

Puede explorar un archivo para la integridad estructural si se realiza una comprobación de archivado. Esta comprobación verifica la presencia de todos los archivos necesarios en el archivado. Para realizar una comporbación de archivado, siga los pasos que se indican en el siguiente procedimiento:

1. En la Core Console, haga clic en la pestaña **Tools (Herramientas)**.
2. En la opción de **archivado** , haga clic en **Check Archive (Comprobar archivado)**.

   Aparecerá el cuadro de diálogo **Check Archive (Comprobar archivado)**.
3. Seleccione una de las opciones siguientes en la lista desplegable:
   - Local: Output location (Local: ubicación de salida): introduzca la ubicación de la salida. Se define la ruta de acceso de ubicación en la que desea que resida el archivo.
   - Network (Red)
     - Output location (Ubicación de salida): introduzca la ubicación de la salida. Se define la ruta de acceso de ubicación en la que desea que resida el archivo.
     - User Name (Nombre de usuario): introduzca un nombre de usuario. Se establecen las credenciales de inicio de sesión para el recurso compartido de red.
     - Password (Contraseña): introduzca una contraseña para la ruta de acceso de red. Se establece las credenciales de inicio de sesión para el recurso compartido de red.
   - Cloud (Nube)
     - Account (Cuenta): seleccione una cuenta desde la lista desplegable. Para seleccionar una cuenta de servicios en la nube, debe haberla agregado primero en la Core Console.
     - Container (Contenedor): en el menú desplegable, seleccione un contenedor asociado a la cuenta.
     - Folder Name (Nombre de la carpeta): escriba un nombre para la carpeta en la que se van a guardar los datos archivados. El nombre predeterminado es AppAssure-5-Archive-[FECHA DE CREACIÓN]-[HORA DE CREACIÓN]
4. Para realizar una verificación de integridad de estructura, seleccione **Structure integrity (Integridad de estructura)**.
5. Haga clic en **Check File (Comprobar archivo)**.

Importación de un archivo

Para importar un archivo:

1. En la Core Console, seleccione la pestaña **Configuration (Configuración)**.
2. En la opción **Manage (Administrar)**, haga clic en **Archive (Archivo)** y, a continuación, en **Import (Importar)**.

   Aparecerá el cuadro de diálogo **Import Archive (Importar archivo)**.
3. En el cuadro de diálogo **Import Archive (Importar archivo)**, introduzca los detalles para importar el archivo, según se describe a continuación:

Cuadro de texto	Descripción
Input Location (Ubicación de entrada)	Seleccione la ubicación para la importación del archivo.
Nombre de usuario	Para establecer acceso para proteger el archivo, introduzca las credenciales de inicio de sesión.
Contraseña	Introduzca una contraseña para el archivo.

4. Haga clic en **Check File (Comprobar archivo)** para validar la existencia del archivo que se va a importar.

   Aaprecerá el cuadro de diálogo **Restore (Restaurar)**.
5. En el cuadro de diálogo **Restore (Restaurar)**, verifique el nombre del Core de origen.
6. Seleccione los Agents que se van a importar desde el archivo.
7. Seleccione el repositorio.
8. Haga clic en **Restore (Restaurar)** para importar el archivo.

Administración de la conectabilidad de SQL

La configuración de conectabilidad para SQL permite que el Core conecte una base de datos SQL y archivos de registro a una instantánea de un servidor SQL a través de una instancia local de Microsoft SQL Server. Mediante la prueba de conectabilidad, el Core comprueba la coherencia de las bases de datos SQL y garantiza que todos los archivos de datos (archivos MDF y LDF) estén disponibles en la instantánea de copia de seguridad. Las pruebas de conectabilidad se pueden ejecutar a petición para puntos de recuperación específicos o como parte de tareas nocturnas.

La conectabilidad requiere una instancia local de Microsoft SQL Server en la máquina del AppAssure Core. Esta instancia debe tener instalada una versión completa de SQL Server adquirida de Microsoft o de un distribuidor autorizado. Microsoft no admite el uso de licencias de SQL pasivas.

Por último, la conectabilidad admite SQL Server 2005, 2008, 2008 R2, 2012 y 2014. La cuenta que se use para realizar la prueba debe tener asignada la función sysadmin en la instancia de SQL Server.

El formato de almacenamiento en disco de SQL Server es el mismo en ambos entornos de 64 bits y 32 bits y la conectabilidad funciona entre ambas versiones. Una base de datos que se desconecte de una instancia de servidor ejecutándose en un entorno puede conectarse a una instancia de servidor que se ejecute en otro entorno.

PRECAUCIÓN: La versión de SQL Server en el Core debe ser igual o superior a la versión SQL Server de todos los Agents con SQL Server instalado.

Configuración de los valores de conectabilidad de SQL

Antes de ejecutar comprobaciones de conectabilidad en las bases de datos SQL protegidas, seleccione una instancia local de SQL Server en la máquina del Core que se usará para realizar las comprobaciones con respecto a la máquina del Agent.

NOTA: La conectabilidad requiere una instancia local de Microsoft SQL Server en la máquina del AppAssure Core. Esta instancia debe tener instalada una versión completa de SQL Server adquirida de Microsoft o de un distribuidor autorizado. Microsoft no admite el uso de licencias de SQL pasivas.

Para configurar la conectabilidad de SQL:

1. Vaya a la Core Console. Haga clic en la pestaña.
2. Haga clic en **Configuration (Configuración)** → **Settings (Valores)**.
3. En el área Nightly Jobs (Trabajos nocturnos), haga clic en **Change (Cambiar)**.

   Aparecerá el cuadro de diálogo **Nightly Jobs (Trabajos nocturnos)**.
4. Seleccione **Attachability Check Job (Trabajo de comprobación de conectabilidad)** y, a continuación, haga clic en **Settings (Valores)**.
5. Utilice los menús desplegables para seleccionar la instancia de SQL Server instalada en el Core a partir de las siguientes opciones:

   Puede elegir entre:

   - **SQL Server 2005**
   - **SQL Server 2008**
   - **SQL Server 2008 R2**
   - **SQL Server 2012**
   - **SQL Server 2014**
6. Seleccione el tipo de credencial.

   Puede elegir entre:

   - **Windows**
   - **SQL**
7. Especifique las credenciales con privilegios administrativos para las instancias de Windows o SQL Server, según se describe a continuación:

Cuadro de texto	Descripción
Nombre de usuario	Introduzca un nombre de usuario para los permisos de inicio de sesión en el SQL Server.
Contraseña	Introduzca una contraseña para la conectabilidad de SQL. Se utiliza para controlar la actividad de inicio de sesión.

8. Haga clic en **Test Connection (Probar conexión)**.

   NOTA: Si ha introducido las credenciales incorrectamente, se mostrará un mensaje alertándole de que la prueba de las credenciales ha fallado. Corrija la información de credenciales y ejecute de nuevo la prueba de conexión.
9. Haga clic en **Save (Guardar)**.

   Las comprobaciones de conectabilidad están ahora disponibles para su ejecución en las bases de datos del SQL Server protegido.
10. En la ventana Nightly Jobs (Trabajos nocturnos), haga clic en **OK (Aceptar)**.

    Las comprobaciones de conectabilidad están ahora programadas para llevarse a cabo con los trabajos nocturnos.

Configuración nocturna de las comprobaciones de conectabilidad SQL y el truncamiento de registro

Para configurar las comprobaciones nocturnas de conectabilidad SQL y el truncamiento de registro:

1. En el área de navegación izquierda de Core, seleccione la máquina para la que quiere que se realicen las comprobaciones de conectabilidad nocturnas y el truncamiento de registro y haga clic en **SQL Server Settings (Configuración de SQL Server)**.
2. Vaya a la Core Console.
3. Haga clic en **Configuration (Configuración)** → **Settings (Valores)**.
4. En la sección **Nightly Jobs (Trabajos nocturnos)**, haga clic en **Change (Cambiar)**.
5. Seleccione o borre la configuración siguientes de SQL Server, según las necesidades de su organización:
   - **Attachability Check Job (Trabajo de comprobación de conectabilidad)**
   - **Log Truncation Job (Trabajo de truncamiento de registro)**
6. Haga clic en **OK (Aceptar)**.

   Las configuraciones de conectabilidad y truncamiento de registro serán efectivas para el SQL Server protegido.

Administración de las comprobaciones de capacidad de montaje de la base de datos de Exchange y truncamiento de registro

Cuando se utiliza AppAssure para realizar copias de seguridad de los servidores Microsoft Exchange, pueden realizarse comprobaciones de capacidad de montaje en todas las bases de datos de Exchange después de cada instantánea. Esta característica de detección de corrupción alerta a los administradores sobre errores potenciales y asegura que se recuperen todos los datos en los servidores Exchange satisfactoriamente en caso de error.

NOTA: Las comprobaciones de capacidad de montaje y funciones de truncamiento de registro solo se aplican a Microsoft Exchange 2007, 2010 y 2013. Además, la cuenta del servicio AppAssure Agent debe tener asignado la función de Organizational Administrator (Administrador organizativo) en Exchange.

Configuración de la capacidad de montaje de la base de datos de Exchange y truncamiento de registro

Puede ver, habilitar o deshabilitar la configuración de servidor de bases de datos Exchange, incluida la comprobación de capacidad de montaje automática, la comprobación de suma de comprobación nocturna o el truncamiento de registro nocturno.

Para configurar la capacidad de montaje de la base de datos de Exchange y truncamiento de registro:

1. En el área de navegación izquierda de Core Console, seleccione la máquina en la que desee configurar las comprobaciones de capacidad de montaje y truncamiento de registro.

   Se muestra la pestaña **Summary (Resumen)** para la máquina seleccionada.
2. Haga clic en **Exchange Server Settings (Configuración de Exchange Server)**.

   Se abrirá el cuadro de diálogo **Exchange Server Settings (Configuración de Exchange Server)**.

3. Seleccione o borre la siguiente configuración de Exchange Server según las necesidades de su organización:
   - **Enable automatic mountability check (Habilitar comprobación de capacidad de montaje automático)**
   - **Enable nightly checksum check (Habilitar comprobación de suma de comprobación nocturna)**
   - **Enable nightly log truncation (Habilitar truncamiento de registro nocturno)**
4. Haga clic en **OK (Aceptar)**.

   Las configuraciones de capacidad de montaje y truncamiento de registro surtirán efecto para el Exchange Server protegido.

   NOTA: Para obtener información sobre cómo forzar el truncamiento de registro, ver Cómo forzar el truncamiento de registro .

Cómo forzar una comprobación de la capacidad de montaje

Para forzar una comprobación de capacidad de montaje:

1. En el área de navegación de la izquierda de la Core Console, seleccione la máquina para la que quiera forzar la comprobación de capacidad de montaje y, a continuación, haga clic en la pestaña **Recovery Points (Puntos de recuperación)**.
2. Haga clic en el símbolo **>** junto a un punto de recuperación de la lista para expandir la vista.
3. Haga clic en **Force Mountability Check (Forzar comprobación de capacidad de montaje)**.

   Un mensaje le solicitará forzar la comprobación de capacidad de montaje.
4. Haga clic en **Yes (Sí)**.

   NOTA: Para obtener instrucciones sobre cómo ver el estado de las comprobaciones de conectabilidad, consulte Visualización de eventos y alertas.

   El sistema realiza la comprobación de capacidad de montaje.

Cómo forzar comprobaciones de suma de comprobación

Para forzar una comprobación de suma de comprobación:

1. En el área de navegación izquierda de la Core Console, seleccione la máquina para la que quiere forzar la comprobación de suma de comprobación y, a continuación, haga clic en la pestaña **Recovery Points (Puntos de recuperación)**.
2. Haga clic en el símbolo **>** junto a un punto de recuperación de la lista para expandir la vista.
3. Haga clic en **Force Checksum Check (Forzar comprobación de suma de comprobación)**.

   La ventana **Force Attachability Check (Forzar comprobación de capacidad de conexión)** le solicita que indique si desea forzar una comprobación de suma de comprobación.
4. Haga clic en **Sí**.

   El sistema realiza la comprobación de suma de comprobación.

   NOTA: Para obtener información sobre cómo ver el estado de las comprobaciones de conectabilidad, consulte Visualización de eventos y alertas.

Cómo forzar el truncamiento de registro

NOTA: Esta opción solo está disponible para máquinas Exchange o SQL.

Para forzar el truncamiento de registro:

1. Vaya a la Core Console y seleccione la pestaña **Machines (Máquinas)**.
2. En la pestaña **Machines (Máquinas)**, realice una de las acciones siguientes:
   - Haga clic en el hiperenlace de la máquina para la que desea truncar el registro.
   - O bien, en el panel de navegación, seleccione la máquina para la que desea truncar el registro.
3. En el menú desplegable **Actions (Acciones)** de esa máquina, haga clic en **Force Log Truncation (Forzar truncamiento de registro)**.
4. Confirme si continuar con el forzado del truncamiento de registro.

Indicadores de estado de punto de recuperación

Después de haber creado un punto de recuperación en un servidor de SQL o Exchange protegido, la aplicación aparece con su correspondiente indicador de estado de color en la tabla **Recovery Points (Puntos de recuperación)**. El color que aparece varía en función de la configuración de comprobación de la máquina protegida y del éxito o no de dichas comprobaciones, tal como se describe en las siguientes tablas.

NOTA: Para obtener más información sobre la visualización de los Puntos de recuperación, consulte Visualización de puntos de recuperación.

La siguiente tabla muestra los indicadores de estado de las bases de datos SQL.

Tabla 2. Colores de punto de estado de recuperación para bases de datos SQL

Color de estado	Descripción
Blanco	Indica que se da una de las condiciones siguientes: • Una base de datos SQL no existe • Las comprobaciones de conectabilidad no estaban habilitadas • Las comprobaciones de conectabilidad aún no se han ejecutado.
Amarillo	Indica que la base de datos SQLestaba fuera de línea y la comprobación no ha sido posible.
Rojo	Indica que la comprobación de conectabilidad ha sido incorrecta.
Verde	Indica que la comprobación de conectabilidad ha sido correcta.

La siguiente tabla muestra los indicadores de estado de las bases de datos Exchange.

Tabla 3. Colores de punto de estado de recuperación para bases de datos de Exchange

Color de estado	Descripción
Blanco	Indica que se da una de las condiciones siguientes: • Una base de datos de Exchange no existe. • Las comprobaciones de capacidad de montaje no estaban habilitadas.

Color de estado	Descripción
	NOTA: Esto se puede aplicar a determinados volúmenes dentro de un punto de recuperación.
Amarillo	Indica que las comprobaciones de capacidad de montaje de base de datos de Exchange están habilitadas, pero las comprobaciones aún no se han ejecutado.
Rojo	Indica que las comprobaciones de capacidad de montaje o de suma de comprobación han sido erróneas en al menos una base de datos.
Verde	Indica que la comprobación de capacidad de montaje o de suma de comprobación ha sido correcta.

NOTA: Los puntos de recuperación que no tengan una base de datos de Exchange o SQL asociada con ellos aparecen con un indicador de estado blanco. En situaciones en las que exista una base de datos de Exchange y una base de datos SQL para el punto de recuperación, aparece el indicador de estado más grave para el punto de recuperación.

3

Administración del appliance DL4000

En la Core Console se incluye la pestaña **Appliance**, que permite aprovisionar espacio, supervisar el estado del servidor y acceder a herramientas de administración.

Supervisión del estado del appliance DL4000

Puede supervisar el estado de los subsistemas del appliance DL4000 mediante la pestaña **Appliance** de la página **Overall Status (Estado general)**. En la página **Overall Status (Estado general)** se muestra un indicador de estado al lado de cada subsistema, junto con una descripción que indica el estado de condición del subsistema.

En esta página también se incluyen enlaces a herramientas que permiten conocer más detalles de los subsistemas, y resultan muy útiles a la hora de solucionar problemas relacionados con advertencias o errores. Al hacer clic en el enlace **System Administrator (Administrador del sistema)**, disponible para los subsistemas de Hardware del appliance y Hardware de almacenamiento, se le solicitará que inicie sesión en la aplicación de Administrador del sistema que se usa para administrar el hardware. Para obtener más información acerca de la aplicación Administrador del sistema, consulte la *Guía del usuario de OpenManage Server Administrator* disponible en **dell.com/support/home**. El enlace **Provisioning Status (Estado de aprovisionamiento)**, disponible para el subsistema de aprovisionamiento de almacenamiento, abre la pantalla **Tasks (Tareas)**, que muestra el estado de aprovisionamiento de ese subsistema. Si hay almacenamiento disponible para aprovisionar, aparece un enlace **Provision (Aprovisionar)** debajo de **Actions (Acciones)** al lado de la tarea de aprovisionamiento.

Aprovisionamiento de almacenamiento

El servidor configura el almacenamiento interno DL4000 disponible y cualquier gabinete de almacenamiento externo adjunto para:

- Repositorios AppAssure

  NOTA: Si se configura el HBA de canal de fibra, el proceso de creación de los repositorios es manual. AppAssure no creará un repositorio automáticamente en el directorio raíz. Para obtener más información, consulte la *Dell DL4000 Appliance Deployment Guide (Guía de implementación del appliance Dell DL4000)*.
- Modo de espera virtual de sistemas protegidos

NOTA: Se admiten MD1200 con unidades de 1 TB, 2 TB, 3 TB o 4 TB (para capacidad alta) conectadas a la controladora H810. Se admiten hasta cuatro MD1200.

NOTA: La configuración de alta capacidad de DL4000 admite un adaptador SAS PERC H810 o dos HBA de Fibre Channel. Para obtener más información acerca de la configuración de HBA de Fibre Channel, consulte el documento técnico *DL4xxx — Fibre Channel Implementation (DL4xxx: Implementación de Fibre Channel)* en **dell.com/support/home**.

Antes de empezar a aprovisionar almacenamiento en el disco, establezca la cantidad de almacenamiento deseada para las máquinas virtuales en espera. Puede asignar cualquier porcentaje de la capacidad disponible para alojar máquinas virtuales en espera. Por ejemplo, si va a usar la administración de recursos de almacenamiento (SRM), puede asignar hasta el 100 por cien de la capacidad de cualquier dispositivo aprovisionado para alojar máquinas virtuales. Con la función de Recuperación directa de AppAssure, puede usar estas máquinas virtuales para reemplazar fácilmente cualquier servidor erróneo que proteja el DL4000.

Gracias a un entorno de tamaño medio que no necesita máquinas virtuales en espera, puede usar todo el almacenamiento para realizar copias de seguridad de un número considerable de Agents. No obstante, si precisa más recursos para las máquinas virtuales en espera y tiene que realizar copias de seguridad de un número menor de máquinas de Agent, puede asignar más recursos para máquinas virtuales más grandes.

Al seleccionar la pestaña **Appliance**, el software de servidor AppAssure detecta el espacio de almacenamiento disponible para todas las controladoras compatibles con el sistema y verifica que el hardware cumpla los requisitos.

Para completar al aprovisionamiento de discos del almacenamiento disponible:

1. En la pestaña **Appliance**, haga clic en **Tasks (Tareas)**.

   En la pantalla **Tasks (Tareas)** se muestra la capacidad de almacenamiento interno del servidor. Esta capacidad se usa para crear un nuevo repositorio de AppAssure.

   PRECAUCIÓN: Antes de proceder, asegúrese de seguir del paso 2 al 4 en este procedimiento.
2. Abra la ventana **Provisioning Storage (Aprovisionamiento de almacenamiento)** haciendo clic en **Provision (Aprovisionar)** en la columna Action (Acción) junto al almacenamiento que desee aprovisionar.
3. En la sección **Provisioning Task Action (Acción de tareas de aprovisionamiento)**, asegúrese de que la casilla de verificación situada junto a **Do this for only one provisioning task when more than one task is being provisioned at a time (Haga esto solo para una tarea de aprovisionamiento cuando se esté aprovisionando a más de una tarea a la vez)** está seleccionada, a menos que desee tener una reserva en el primer gabinete (en cuyo caso, mantendría ese valor seleccionado).
4. En la sección **Optional Storage Reserve (Reserva de almacenamiento opcional)**, seleccione la casilla de verificación junto a **Allocate a portion of the storage being provisioned for Standby Virtual Machines or other purposes (Asignar una parte del almacenamiento que se está aprovisionando para máquinas virtuales en espera o para otros fines)** e indique el porcentaje de almacenamiento que se va a asignar. De lo contrario, el porcentaje de almacenamiento que se indica en la sección **Optional Storage Reserve (Reserva de almacenamiento opcional)** se eliminará de todos los discos conectados.
5. Haga clic en **Provision All (Aprovisionar todo)**.

   NOTA: Si, por ejemplo, decide asignar el 30 por ciento del almacenamiento a máquinas virtuales en espera, el comando **Provision All (Aprovisionar todo)** aprovisionará el almacenamiento interno en una proporción del 70 por ciento al repositorio y del 30 por ciento a las máquinas virtuales en espera. Si no activó la casilla **Do this for only one provisioning task when more than one task is being provisioned at a time (Realizar esta acción para una sola tarea de aprovisionamiento cuando se esté aprovisionando más de una tarea a la vez)**, el 100 por cien del almacenamiento externo se aprovisionará al repositorio, y se agregará como espacio de almacenamiento adicional para el repositorio que se está creando en el almacenamiento interno.

Aprovisionamiento del almacenamiento seleccionado

Para aprovisionar el almacenamiento seleccionado:

1. En la pestaña **Appliance**, haga clic en **Tasks (Tareas)**.

   La pantalla **Tasks (Tareas)** muestra la capacidad de almacenamiento interno y externo del servidor, con independencia de si está disponible para aprovisionarse o ya se ha aprovisionado, o de si existe alguna condición que evite que el almacenamiento se aprovisione automáticamente. Esta capacidad se usa para crear un repositorio de AppAssure.
2. Para aprovisionar solo una parte del espacio disponible, haga clic en **Provision (Aprovisionar)** en **Action (Acción)** junto al espacio de almacenamiento que desee aprovisionar.
   - Para crear un repositorio nuevo, seleccione **Create a new repository (Crear un repositorio nuevo)**, y especifique un nombre para el repositorio.

     De manera predeterminada, aparece Repository 1 (Repositorio 1) como nombre del repositorio. Puede sobrescribir el nombre si lo desea.
   - Para agregar capacidad a un repositorio existente, seleccione **Expand the existing repository (Ampliar el repositorio existente)** y, a continuación, elija el repositorio en la lista **Existing Repositories (Repositorios existentes)**.

   NOTA: Para agregar capacidad, se recomienda que amplíe un repositorio existente en lugar de agregar uno nuevo. Los repositorios independientes no utilizan la capacidad con la misma eficiencia, ya que en ellos no tiene lugar la desduplicación.
3. En **Optional Storage Reserve (Reserva de almacenamiento opcional)**, puede seleccionar la opción para asignar parte del almacenamiento para máquinas virtuales en espera y, a continuación, especificar el porcentaje de almacenamiento que se va a asignar a las máquinas virtuales.
4. También puede desactivar la casilla **Do this for only one provisioning task when more than one task is being provisioned at a time (Realizar esta acción para una sola tarea de aprovisionamiento cuando se esté aprovisionando más de una tarea a la vez)** (seleccionada de manera predeterminada).

   Al desactivar esta opción, el porcentaje de almacenamiento elegido se aplica solo al dispositivo de almacenamiento seleccionado. Si selecciona esta opción, podrá aplicar el porcentaje de almacenamiento elegido a los gabinetes de almacenamiento interno y externo.
5. Haga clic en **Provision (Aprovisionar)**.

   Se inicia el aprovisionamiento de discos y el estado de creación del repositorio de AppAssure aparece en el área **Status (Estado)** de la pantalla **Tasks (Tareas)**. La **Status Description (Descripción de estado)** aparece como **Provisioned (Aprovisionado)**.
6. Para ver los detalles después de finalizar el aprovisionamiento de discos, haga clic en el símbolo **>** junto al indicador de estado.

   Se expande la página **Tasks (Tareas)** y muestra el estado, el repositorio y los detalles de discos virtuales (si están asignados).

Eliminación de asignación de espacio para un disco virtual

Antes de empezar este procedimiento, defina los discos virtuales que puede eliminar. En la Core Console, seleccione la pestaña **Appliance**, haga clic en **Tasks (Tareas)** y, a continuación, expanda el repositorio que contiene los discos virtuales para ver su información.

Para eliminar asignación de espacio para un disco virtual:

1. En la aplicación OpenManage Server Administrator, expanda la opción **Storage (Almacenamiento)**.
2. Expanda la controladora que contiene el disco virtual y, a continuación, seleccione **Virtual Disks (Discos virtuales)**.
3. Seleccione el disco virtual que desea quitar y elija **Delete (Eliminar)** en el menú desplegable **Tasks (Tareas)**.
4. Después de confirmar la eliminación, el espacio aparecerá como disponible para el aprovisionamiento en la pestaña **Appliance** de la pantalla **Tasks (Tareas)** de la Core Console.

Resolución de tareas erróneas

AppAssure notifica las tareas de comprobación de aprovisionamiento y de recuperación erróneas de un evento en la página principal de la Core Console, así como en la pestaña **Appliance** de la pantalla **Tasks (Tareas)**.

Para ver cómo solucionar una tarea errónea, seleccione la pestaña **Appliance** y haga clic en **Tasks (Tareas)**. Expanda la tarea errónea haciendo clic en el símbolo **>**, que aparece junto a **Status (Estado)**, y revise el mensaje de error y la acción recomendada.

Actualización del appliance DL4000

Antes de comenzar el proceso de actualización, asegúrese de detener los servicios del Core.
Para actualizar el appliance DL4000:

1. Descargue la **Recovery and Update Utility (Utilidad de recuperación y actualización)** desde **dell.com/support** en el servidor de copia de seguridad en disco DL4000.
2. Copie la utilidad al escritorio del servidor y extraiga los archivos.
3. Haga doble clic en el icono **Launch-RUU (Abrir-RUU)**.
4. Cuando se le solicite, haga clic en **Yes (Sí)** para aceptar que no está ejecutando ninguno de los procesos enumerados.
5. Cuando aparezca la pantalla de la **Recovery and Update Utility (Utilidad de recuperación y actualización)**, haga clic en **Start (Inicio)**.
6. Cuando se le solicite reiniciar, haga clic en **OK (Aceptar)**.

   Las versiones actualizadas de funciones y características de Windows Server, ASP .NET MVC3, proveedor de LSI, aplicaciones DL, OpenManage Server Administrator y del software AppAssure Core se instalan como parte de la utilidad de recuperación y actualización.

   NOTA: Además, como parte del proceso de actualización del software AppAssure Core, la utilidad de recuperación y actualización le informa acerca de la versión de AppAssure que está instalada actualmente y le solicita que confirme que desea actualizar el software de Core a la versión integrada en la utilidad. No se admiten degradaciones a versiones anteriores del software de AppAssure.
7. Reinicie el sistema, si se le solicita.
8. Haga clic en **Proceed (Continuar)** cuando todos los servicios y aplicaciones estén instalados.

   La Core Console se inicia.

Reparación del appliance DL4000

Antes de comenzar el proceso de reparación, asegúrese de detener los servicios del Core.

Para reparar el appliance DL4000:

1. Descargue la **Recovery and Update Utility (Utilidad de recuperación y actualización)** de la página **dell.com/support** al appliance DL4000.
2. Copie la utilidad al escritorio del servidor y extraiga los archivos.
3. Haga doble clic en el icono **Launch-RUU (Abrir-RUU)**.
4. Cuando se le solicite, haga clic en **Yes (Sí)** para aceptar que no está ejecutando ninguno de los procesos enumerados.
5. Cuando aparezca la pantalla de la utilidad de recuperación y actualización, haga clic en **Start (Inicio)**.
6. Cuando se le solicite reiniciar, haga clic en **OK (Aceptar)**.

   Las versiones actualizadas de funciones y características de Windows Server, ASP .NET MVC3, proveedor de LSI, aplicaciones DL, OpenManage Server Administrator y del software AppAssure Core se instalan como parte de la utilidad de recuperación y actualización.
7. Si la versión integrada de la utilidad es la misma que la versión instalada, la utilidad de recuperación y actualización le solicitará que confirme si desea ejecutar una instalación de reparación. Este paso se puede omitir si no se necesita una instalación de reparación en el AppAssure Core.
8. Si la versión integrada de la utilidad es superior a la versión instalada, la utilidad de recuperación y actualización le solicitará que confirme si desea actualizar el software de AppAssure Core.

   NOTA: No se admiten degradaciones a versiones anteriores de AppAssure Core.
9. Reinicie el sistema, si se le solicita.
10. Haga clic en **Proceed (Continuar)** cuando todos los servicios y aplicaciones estén instalados.

    La Core Console se inicia.

4

Protección de estaciones de trabajo y servidores

Acerca de la protección de estaciones de trabajo y servidores

Para proteger sus datos agregue las estaciones de trabajo y los servidores que desea proteger en la Core Console; por ejemplo, el servidor de Exchange, SQL Server o el servidor de Linux.

NOTA: En este capítulo, el término *máquina* también se refiere en general al software del Agent instalado en esa máquina.

En la Core Console, puede identificar la máquina en la que está instalado un Agent y especificar qué volúmenes proteger, definir programas para la protección, agregar medidas de seguridad adicionales como el cifrado, etc. Para obtener más información sobre cómo acceder a la Core Console para proteger estaciones de trabajo y servidores, consulte Cómo proteger una máquina.

Configuración de los valores de la máquina

Una vez agregada la protección para las máquinas en AppAssure, puede modificar los valores básicos de configuración de la máquina (como el nombre y el nombre de host), la configuración de protección (cambiar la programación de protección para los volúmenes en la máquina, agregando o quitando volúmenes, o pausando la protección), etc.

Visualización y modificación de los valores de configuración

Para ver y modificar valores de configuración:

1. Una vez agregada una máquina protegida, realice una de las acciones siguientes:
   - En la Core Console, haga clic en la pestaña **Machines (Máquinas)** y, a continuación, haga clic en el hiperenlace de la máquina que desea modificar.
   - En el panel **Navigation (Navegación)**, seleccione la máquina que desea modificar.
2. Haga clic en la pestaña **Configuration (Configuración)**.
   Se abrirá la página **Settings (Valores)**.
3. Haga clic en **Edit (Editar)** para modificar la configuración de la máquina, según se muestra en la tabla siguiente.

Cuadro de texto	Descripción
Nombre de visualización	Introduzca el nombre de visualización de la máquina.

Cuadro de texto	Descripción
	Un nombre para esta máquina que se mostrará en la Core Console. De forma predeterminada, es el nombre del host de la máquina. Puede cambiarlo por un nombre más fácil de identificar si lo desea.
Nombre del host	Introduzca el nombre del host de la máquina.
Port	Introduzca un número de puerto para la máquina. El Core usa este puerto para comunicarse con la máquina.
Repository (Repositorio)	Seleccione un repositorio para los puntos de recuperación. Muestra el repositorio en el Core donde se almacenarán los datos de esta máquina. NOTA: Este valor solo se puede cambiar si no hay puntos de recuperación o si falta el repositorio anterior.
Encryption Key (Clave de cifrado)	Edite la clave de cifrado si es necesario. Especifique si el cifrado se aplica a los datos de cada volumen de esta máquina que se almacenarán en el repositorio.

Visualización de la información del sistema de una máquina

La Core Console proporciona una vista rápida de todas las máquinas que se están protegiendo e incluye una lista de las máquinas, así como su estado.

Para ver la información del sistema de una máquina:

1. En la Core Console, bajo **Protected Machines (Máquinas protegidas)**, seleccione la máquina para la que desea ver información detallada del sistema.
2. Haga clic en la pestaña **Tools (Herramientas)** de la máquina.

   La información sobre la máquina se muestra en la página **System Information (Información del sistema)**. A continuación, se describen los detalles que se incluyen:

   - Nombre del host
   - Versión del SO
   - Arquitectura del SO
   - Memoria (física)
   - Nombre de visualización
   - Nombre de dominio completo
   - Tipo de máquina virtual (si procede)

   La información detallada sobre los volúmenes contenidos en esta máquina incluye:

   - Nombre
   - Id. de dispositivo
   - Sistema de archivos
   - Capacidad (incluida nativa, formateada y usada)
   - Procesadores
   - Tipo de procesadores
   - Adaptadores de red
   - Direcciones IP asociadas con esta máquina

Configuración de grupos de notificación para eventos del sistema

En AppAssure, puede configurar cómo se informa de los eventos del sistema para su máquina mediante la creación de grupos de notificación, entre los que se incluyen alertas del sistema, errores, etc.

Para configurar los grupos de notificación de eventos del sistema:

1. En la Core Console, haga clic en la pestaña **Machines (Máquinas)**.
2. En la pestaña **Machines (Máquinas)**, realice una de las acciones siguientes:
   - Haga clic en el hiperenlace de la máquina que desea modificar.
   - En el panel de navegación, seleccione la máquina que desea modificar.

   Aparece la pestaña **Summary (Resumen)**.
3. Seleccione la pestaña **Configuration (Configuración)** y, a continuación, haga clic en **Events (Eventos)**.

   Aparecerá la página **Notification Groups (Grupos de notificación)**.
4. Haga clic en **Use custom alert settings (Usar configuración de alertas personalizada)** y, a continuación, haga clic en **Apply (Aplicar)**.

   Aparecerá la pantalla **Custom Notification Groups (Grupos de notificación personalizada)**.
5. Haga clic en **Add Group (Agregar grupo)** para agregar nuevos grupos de notificación para enviar una lista de eventos del sistema.

   Se abrirá el cuadro de diálogo **Add Notification Group (Agregar grupo de notificación)**.

   NOTA: Para utilizar la configuración de alerta predeterminada, seleccione la opción **Use Core alert settings (Usar configuración de alerta del Core)**.
6. Agregue las opciones de notificación según se describe en la tabla siguiente.

Cuadro de texto	Descripción
Nombre	Introduzca un nombre para el grupo de notificación.
Descripción	Introduzca una descripción del grupo de notificación.
Enable Events (Habilitar eventos)	Seleccione los eventos a compartir con este grupo de notificación. Puede seleccionar **All (Todo)** o seleccionar un subconjunto de eventos a incluir: • **BootCd** • **LocalMount** • **Metadata** • **Clusters** • **Notification (Notificación)** • **PowerShellScripting** • **PushInstall** • **Attachability** • **Trabajos** • **Licencias** • **LogTruncation** • **Archive** • **Core Service** • **Exportar**

Cuadro de texto	Descripción
	• **Protection** • **Replicación** • **Rollback** • **Rollup** También puede seleccionar por tipo: • **Informativa** • **Aviso** • **Error** NOTA: Si elige seleccionar por tipo, de manera predeterminada, los eventos correspondientes se habilitarán de forma automática. Por ejemplo, si elige Warning(Aviso), se habilitarán los eventos Attachability, Jobs, Licensing, Archive, CoreService, Export, Protection, Replication y Rollback.
Notification Options (Opciones de notificación)	Seleccione el método para especificar cómo administrar notificaciones. Puede elegir entre las siguientes opciones: • **Notify by Email (Notificar por correo electrónico**: especifique a qué direcciones de correo electrónico enviar los eventos en los campos To (Para), CC y, opcionalmente, BCC (CCO). NOTA: Para recibir correo electrónico, debe haber configurado el SMTP previamente. • **Notify by Windows Event log (Notificar por registro de eventos de Windows)**:el registro de eventos de Windows controla la notificación. • **Notify by syslogd (Notificar por syslogd)**: especifique a qué nombre del host y puerto enviar los eventos. – **Host**:introduzca el nombre de host del servidor. – **Port (Puerto)**: introduzca un número de puerto para comunicarse con el servidor.

7. Haga clic en **OK (Aceptar)** para guardar los cambios.
8. Para editar un grupo de notificación existente, haga clic en **Edit (Editar)** junto al grupo de notificación que desee editar.

   Se abre el cuadro de diálogo **Edit Notification Group (Editar grupo de notificación)** donde podrá editar la configuración.

Edición de los grupos de notificación para eventos del sistema

Para editar los grupos de notificación para eventos del sistema

1. Vaya a la Core Console y seleccione la pestaña **Machines (Máquinas)**.
2. En la pestaña **Machines (Máquinas)**, realice una de las acciones siguientes:
   - Haga clic en el hiperenlace de la máquina que desea modificar.
   - O bien, en el panel de navegación, seleccione la máquina que desea quitar.

   Aparece la pestaña **Summary (Resumen)**.
3. Seleccione la pestaña **Configuration (Configuración)** y, a continuación, haga clic en **Events (Eventos)**.

4. Haga clic en **Use custom alert settings (Usar configuración de alertas personalizada)** y, a continuación, haga clic en **Apply (Aplicar)**.

   Aparecerá la pantalla **Custom Notification Groups (Grupos de notificación personalizada)**.

5. Haga clic en el icono **Edit (Editar)** debajo de la columna **Action (Acción)**.

   Aparecerá el cuadro de diálogo **Edit Notification Group (Editar grupo de notificación)**.

6. Edite las opciones de notificación como se describe en la tabla siguiente.

Cuadro de texto	Descripción
Nombre	Representa el nombre del grupo de notificación. NOTA: No puede editar el nombre del grupo de notificación.
Descripción	Introduzca una descripción del grupo de notificación.
Enable Events (Habilitar eventos)	Seleccione qué eventos compartir con el grupo de notificación, Puede seleccionar **All (Todo)** o seleccionar un subconjunto de eventos que incluir: • **BootCd** • **LocalMount** • **Metadata** • **Clusters** • **Notification (Notificación)** • **PowerShellScripting** • **PushInstall** • **Attachability** • **Trabajos** • **Licencias** • **LogTruncation** • **Archive** • **Core Service** • **Exportar** • **Protection** • **Replicación** • **Rollback** • **Rollup** También puede seleccionar por tipo: • **Informativa** • **Aviso** • **Error** NOTA: Si elige seleccionar por tipo, de manera predeterminada, los eventos correspondientes se habilitarán de forma automática. Por ejemplo, si elige Warning(Aviso), se habilitarán los eventos Attachability, Jobs, Licensing, Archive, CoreService, Export, Protection, Replication y Rollback.

Cuadro de texto	Descripción
Notification Options (Opciones de notificación)	Seleccione el método para especificar cómo administrar notificaciones. Puede elegir entre las siguientes opciones: • **Notify by Email (Notificar por correo electrónico)**: especifique a qué direcciones de correo electrónico enviar los eventos en los campos To (Para), CC y BCC (CCO). NOTA: Para recibir correo electrónico, debe haber configurado previamente el SMTP. • **Notify by Windows Event log (Notificar por registro de eventos de Windows)**:el registro de eventos de Windows controla la notificación. • **Notify by syslogd (Notificar por syslogd)**: especifique a qué nombre del host y puerto enviar los eventos. – **Host**:introduzca el nombre de host del servidor. – **Port (Puerto)**: introduzca un número de puerto para comunicarse con el servidor.

7. Haga clic en **OK (Aceptar)**.

Personalización de la configuración de la política de retención

La política de retención para una máquina especifica durante cuánto tiempo se almacenan los puntos de recuperación para una máquina Agent en el repositorio. Las políticas de retención se utilizan para retener instantáneas de copia de seguridad durante periodos de tiempo más largos y para ayudar a administrar estas instantáneas de copia de seguridad. Mediante un proceso de mantenimiento periódico se aplica la política de retención, que ofrece asistencia con copias de seguridad obsoletas y en la eliminación de copias de seguridad antiguas. Esta tarea también es un paso en Proceso para la modificación de la configuración del nodo de clúster.

Para personalizar la configuración de la política de retención:

1. En la Core Console, haga clic en la pestaña **Machines (Máquinas)**.
2. En la pestaña **Machines (Máquinas)**, realice una de las acciones siguientes:
   - Haga clic en el hiperenlace de la máquina que desea modificar.
   - En el panel de navegación, seleccione la máquina que desea modificar.

   Aparece la pestaña **Summary (Resumen)**.
3. Seleccione la pestaña **Configuration (Configuración)** y, a continuación, haga clic en **Retention Policy (Política de retención)**.

   NOTA: Para utilizar la política de retención predeterminada configurada para el Core, asegúrese de que se ha seleccionado la opción Use Core default retention policy (Utilizar la política de retención predeterminada del Core).

   Aparece la pantalla **Retention Policy (Política de retención)**.
4. Para establecer las políticas personalizadas, haga clic en **Use custom retention policy (Utilizar la política de retención personalizada)**.

   Aparece la pantalla **Custom Retention Policy (Política de retención personalizada)**.
5. Seleccione **Enable Rollup (Habilitar mantenimiento períodico)**, y especifique los intervalos de tiempo que se retendrán los datos de copia de seguridad según sea necesario. Las opciones de la política de retención se describen a continuación:

Cuadro de texto	Descripción
Keep all recovery points for n [retention time period] (Conservar todos los puntos de recuperación durante n [período de tiempo de retención])	Especifica el período de retención de los puntos de recuperación. Introduzca el número que represente el período de retención y seleccione el período de tiempo. El valor predeterminado es **3**. Puede elegir entre: • **Days (Días)** • **Weeks (Semanas)** • **Months (Meses)** • **Years (Años)**
...and then keep one recovery point per hour for n [retention time period] (...y luego conservar un punto de recuperación por hora durante n [período de tiempo de retención])	Proporciona un nivel de retención más detallado. Se utiliza como bloque de construcción con la configuración primaria para definir con más detalle durante cuánto tiempo se mantienen los puntos de recuperación. Introduzca el número que represente el período de retención y seleccione el período de tiempo. El valor predeterminado es 2. Puede elegir entre: • **Days (Días)** • **Weeks (Semanas)** • **Months (Meses)** • **Years (Años)**
..and then keep one recovery point per day for n [retention time period] (...y luego conservar un punto de recuperación por día durante n [período de tiempo de retención])	Proporciona un nivel de retención más detallado. Se utiliza como bloque de construcción para definir con más detalle durante cuánto tiempo se mantienen los puntos de recuperación. Introduzca el número que represente el período de retención y seleccione el período de tiempo. El valor predeterminado es 4. Puede elegir entre: • **Days (Días)** • **Weeks (Semanas)** • **Months (Meses)** • **Years (Años)**
...and then keep one recovery point per week for n [retention time period] (...y luego conservar un punto de recuperación por semana durante n [período de	Proporciona un nivel de retención más detallado. Se utiliza como bloque de construcción para definir con más detalle durante cuánto tiempo se mantienen los puntos de recuperación. Introduzca el número que represente el período de retención y seleccione el período de tiempo. El valor predeterminado es 3. Puede elegir entre: • **Weeks (Semanas)** • **Months (Meses)**

Cuadro de texto	Descripción
tiempo de retención])	• **Years (Años)**
..and then keep one recovery point per month for n [retention time period] (...y luego conservar un punto de recuperación por mes durante n [período de tiempo de retención])	Proporciona un nivel de retención más detallado. Se utiliza como bloque de construcción para definir con más detalle durante cuánto tiempo se mantienen los puntos de recuperación. Introduzca el número que represente el período de retención y seleccione el período de tiempo. El valor predeterminado es 2. Puede elegir entre: • **Months (Meses)** • **Years (Años)**
...and then keep one recovery point per year for n [retention time period] (...y luego conservar un punto de recuperación por año durante n [período de tiempo de retención])	Introduzca el número que represente el período de retención y seleccione el período de tiempo.

El cuadro de texto Newest Recovery Point (Punto de recuperación más reciente) muestra el punto de recuperación más reciente. La configuración de la política de retención establece el punto de recuperación más antiguo.

En el ejemplo siguiente se explica cómo se calcula el período de retención.

Conservar todos los puntos de recuperación durante 3 días.

...y luego conservar un punto de recuperación por hora durante 3 días

...y luego conservar un punto de recuperación por día durante 4 días

...y luego conservar un punto de recuperación por semana durante 3 semanas

...y luego conservar un punto de recuperación por mes durante 2 meses

....y luego conservar un punto de recuperación por mes durante 1 año

La opción Newest Recovery Point (Punto de recuperación más reciente) se establece en el día, mes y año actuales.

En este ejemplo, el punto de recuperación más antiguo puede tener un año, cuatro meses y seis días de antigüedad.

6. Haga clic en **Apply (Aplicar)** para guardar los cambios.
7. Seleccione **Force Rollup (Forzar mantenimiento periódico)** para realizar un mantenimiento período en base a la política de retención actual para la máquina, o permitir que la política de retención definida se aplique durante el mantenimiento período nocturno.

Visualización de la información de la licencia

Puede ver la información sobre el estado actual de la licencia del software de Agent de AppAssure instalado en una máquina.

Para ver la información de la licencia:

1. En la Core Console, haga clic en la pestaña **Machines (Máquinas)**.
2. En la pestaña **Machines (Máquinas)**, realice una de las acciones siguientes:
   - Haga clic en el hiperenlace de la máquina que desea ver.
   - En el panel de navegación, seleccione la máquina que desea ver.
3. Haga clic en la pestaña **Configuration (Configuración)** y, a continuación, haga clic en **Licensing (Licencias)**.

   La pantalla **Status (Estado)** muestra los detalles sobre la licencia del producto.

Modificación de los programas de protección

En AppAssure puede modificar los programas de protección de volúmenes específicos de una máquina.

Para modificar los programas de protección:

1. En la Core Console, haga clic en la pestaña **Machines (Máquinas)**.
2. En la pestaña **Machines (Máquinas)**, realice una de las acciones siguientes:
   - Haga clic en el hiperenlace de la máquina que desea modificar.
   - En el panel de navegación, seleccione la máquina que desea modificar.
3. Realice uno de los siguientes pasos:
   - En la tabla **Volumes (Volúmenes)** de la pestaña **Summary (Resumen)** de la máquina, haga clic en el hiperenlace del programa de protección del volumen que desea personalizar.
   - Haga clic en la pestaña **Configuration (Configuración)** y, a continuación, haga clic en **Protection Settings (Configuración de protección)**. En la lista de volúmenes, haga clic en el icono **Edit (Editar)** situado junto al volumen que desea personalizar.

   Aparecerá el cuadro de diálogo **Protection Schedule (Programa de protección)**.
4. En el cuadro de diálogo **Protection Schedule (Programa de protección)**, edite las siguientes opciones de programa según sea necesario para proteger sus datos. La siguiente tabla describe las opciones.

Opción	Descripción
Interval (Intervalo)	**Weekday (Día de la semana)**: para proteger los datos en un intervalo de tiempo específico (p. ej., cada 15 minutos), seleccione **Interval (Intervalo)** y a continuación: • Para personalizar cuándo se protegen los datos durante las horas de máxima actividad, en los menús desplegables puede seleccionar **Start Time (Hora de inicio)**, **End Time (Hora de finalización)** e **Interval (Intervalo)**. • Para proteger los datos fuera del horario de máxima actividad, en el menú desplegable seleccione la casilla de verificación **Protection interval during**

Opción	Descripción
	off-peak times (Protección fuera del horario de máxima actividad) y, a continuación, un intervalo para la protección. **Weekends (Fines de semana)**: para proteger también los datos durante los fines de semana, en el menú desplegable seleccione la casilla de verificación **Protection interval during weekends (Intervalo de protección durante los fines de semana)** y, a continuación, seleccione un intervalo. NOTA: Si las bases de datos y registros de SQL o Exchange están en volúmenes distintos, los volúmenes deben pertenecer a un grupo de protección.
Daily (Diariamente)	Para proteger los datos diariamente, seleccione la opción **Daily (Diario)** y, a continuación, en el menú desplegable **Protection Time (Hora de la protección)** seleccione la hora de inicio de la protección de los datos.
No Protection (Sin protección)	Para eliminar la protección de este volumen, seleccione la opción **No Protection (Sin protección)**.

Si desea aplicar esa configuración personalizada a todos los volúmenes en esa máquina, seleccione **Apply to All Volumes (Aplicar a todos los volúmenes)**.

5. Cuando haya hecho todos los cambios necesarios, haga clic en **OK (Aceptar)**.

Modificación de la configuración de las transferencias

Puede modificar la configuración para administrar procesos de transferencia de datos en una máquina protegida. La configuración de transferencia que se describe en esta sección es a nivel de Agent. Para ver cómo transferir datos en el Core, consulte Modificación de la configuración de la cola de transferencias.

PRECAUCIÓN: La modificación de la configuración de transferencias puede tener graves consecuencias en su entorno. Antes de cambiar los valores de esta configuración, consulte la Transfer Performance Tuning Guide (Guía de configuración para la ejecución de transferencias) en la base de conocimiento de Dell AppAssure https://support.software.dell.com/appassure/kb.

Hay tres tipos de transferencias:

Instantáneas	La transferencia que realiza la copia de seguridad de los datos de la máquina protegida.
Exportación de la VM	Tipo de transferencia que crea una máquina virtual con toda la información y los parámetros de la copia de seguridad según se hayan especificado en el programa definido para proteger la máquina.
Rollback	Un proceso que restaura información de copia de seguridad en una máquina protegida.

La transferencia de datos conlleva la transmisión de un volumen de datos a través de una red desde las máquinas Agent hasta el Core. En caso de replicación, la transferencia también se puede efectuar desde el Core de origen hasta el de destino.

Además, la transferencia de datos se puede optimizar para un sistema mediante una configuración opcional de rendimiento. Esta configuración controla el uso del ancho de banda de los datos durante los procesos de copia de seguridad de máquinas de Agent, y permite realizar exportaciones de MV o

reversiones. Estos son algunos de los factores que influyen en el rendimiento de la transferencia de datos:

- Número de transferencias de datos de Agent simultáneas
- Número de flujos de datos simultáneos
- Número de cambios de datos en el disco
- Ancho de banda de red disponible
- Rendimiento del subsistema del disco del repositorio
- Cantidad de memoria disponible para el almacenamiento en búfer de los datos

Puede ajustar las opciones de rendimiento para que mejor se adapten a sus necesidades empresariales y adaptarlas a su entorno.

Para modificar la configuración de las transferencias:

1. En la Core Console, realice una de las acciones siguientes:
   - Haga clic en la pestaña **Machines (Máquinas)** y, a continuación, en el hiperenlace de la máquina que desea modificar.
   - O bien, en el panel de navegación, haga clic en la máquina que desea modificar.
2. En la pestaña **Machines (Máquinas)**, realice una de las acciones siguientes:
   - Haga clic en el hiperenlace de la máquina que desea modificar.
   - En el panel de navegación, seleccione la máquina que desea modificar.
3. Haga clic en la pestaña **Configuration (Configuración)** y, a continuación, haga clic en **Transfer Settings (Configuración de transferencia)**.

   Aparecerá la configuración de transferencia actual.
4. En la página **Transfer Settings (Configuración de transferencia)**, haga clic en **Change (Cambiar)**.

   Aparecerá el cuadro de diálogo **Transfer Settings (Configuración de transferencia)**.
5. Introduzca las opciones de **Transfer Settings (Configuración de transferencia)** para la máquina como se describe en la tabla siguiente.

Cuadro de texto	Descripción
Prioridad	Establece la prioridad de transferencia entre las máquinas protegidas. Permite asignar la prioridad mediante la comparación con otras máquinas protegidas. Seleccione un número del 1 al 10, siendo el 1 la máxima prioridad. La configuración predeterminada establece una prioridad de 5. NOTA: La prioridad se aplica a las transferencias que hay en la cola.
Maximum Concurrent Streams (Número máximo de transmisiones concurrentes)	Establece el número máximo de enlaces TCP que se envían al Core para el procesamiento paralelo por Agent. NOTA: Dell recomienda establecer este valor en 8. Si experimenta la pérdida de paquetes, pruebe a aumentar el valor.
Maximum Concurrent Writes (Número máximo	Establece el número máximo de acciones de escritura en disco simultáneas por conexión de Agent.

Cuadro de texto	Descripción
de escrituras concurrentes)	NOTA: Dell recomienda establecer este valor en el mismo valor seleccionado para Maximum Concurrent Streams (Número máximo de transmisiones simultáneas). Si experimenta la pérdida de paquetes, elija un valor algo inferior. Por ejemplo, si el número máximo de transmisiones simultáneas está establecido en 8, configure esta opción en 7.
Maximum Retries (Número máximo de reintentos)	Establece el número máximo de reintentos para cada máquina protegida, si algunas de las operaciones no se pueden completar.
Maximum Segment Size (Tamaño máximo de segmento)	Especifica la cantidad máxima de datos, en bytes, que un equipo puede recibir en un único segmento TCP. La configuración predeterminada es 4194304. **PRECAUCIÓN: No cambie la configuración predeterminada de esta opción.**
Maximum Transfer Queue Depth (Profundidad de cola de transferencia máxima)	Especifica el número de comandos que se pueden establecer de manera simultánea. Puede ajustar esta opción en un número más alto si en su sistema se realiza un número elevado de operaciones de entrada/salida simultáneas.
Outstanding Reads per Stream (Lecturas pendientes por flujo)	Especifica el número de operaciones de lectura en cola que se almacenará en el back-end. Esta configuración permite controlar la puesta en cola de los Agents. NOTA: Dell recomienda establecer este valor en 24.
Excluded Writers (Escritores excluidos)	Seleccione un escritor si desea excluirlo. Debido a que los escritores que aparecen en la lista son específicos de la máquina que se está configurando, puede que no aparezcan todos los escritores en la lista. Estos son algunos de los que aparecerán: • ASR Writer (Escritor ASR) • BITS Writer (Escritor BITS) • COM+ REGDB Writer (Escritor COM+ REGDB) • Performance Counters Writer (Escritor de contadores de rendimiento) • Registry Writer (Escritor de registro) • Shadow Copy Optimization Writer (Escritor de optimización de instantáneas) • SQLServerWriter (Escritor SQLServer) • System Writer (Escritor del sistema) • Task Scheduler Writer (Escritor del programador de tareas) • VSS Metadata Store Writer (Escritor del almacén de metadatos de VSS) • WMI Writer (Escritor WMI)

Cuadro de texto	Descripción
Transfer Data Server Port (Puerto de servidor de datos de transferencia)	Configura el puerto para las transferencias. La configuración predeterminada es 8009.
Transfer Timeout (Tiempo de espera de transferencia)	Especifica los minutos y segundos que un paquete puede permanecer como estático sin transferirse.
Snapshot Timeout (Tiempo de espera de instantánea)	Especifica el tiempo máximo de espera, en minutos y segundos, para tomar una instantánea.
Network Read Timeout (Tiempo de espera de lectura de red)	Especifica el tiempo máximo de espera, en minutos y segundos, para una conexión de lectura. Si la lectura de red no se realiza en este tiempo, se vuelve a intentar la operación.
Network Write Timeout (Tiempo de espera de escritura de red)	Especifica el tiempo máximo de espera, en segundos, para una conexión de escritura. Si la escritura de red no se realiza en este tiempo, se vuelve a intentar la operación.

6. Haga clic en **OK (Aceptar)**.

Reinicio de un servicio

Para reiniciar un servicio:

1. En la Core Console, haga clic en la pestaña **Machines (Máquinas)**.
2. En la pestaña **Machines (Máquinas)**, realice una de las acciones siguientes:
   - Haga clic en el hiperenlace de la máquina que desea reiniciar.
   - En el panel **Navigation (Navegación)**, seleccione la máquina que desea reiniciar.
3. Haga clic en la pestaña **Tools (Herramientas)** y, a continuación, haga clic en **Diagnostics (Diagnósticos)**.
4. Seleccione la opción **Restart Service (Reiniciar servicio)** y, a continuación, haga clic en el botón **Restart Service (Reiniciar servicio)**.

Visualización de los registros de la máquina

Si se producen errores o problemas con la máquina, puede ser útil consultar los registros para solucionarlos.

Para ver los registros de la máquina:

1. En la Core Console, haga clic en la pestaña **Machines (Máquinas)**.
2. En la pestaña **Machines (Máquinas)**, realice una de las acciones siguientes:
   - Haga clic en el hiperenlace de la máquina que contenga los registros que desea ver.
   - En el panel **Navigation (Navegación)**, seleccione la máquina que contenga los registros que desea ver.
3. Haga clic en la pestaña **Tools (Herramientas)** y, a continuación, haga clic en **Diagnostics (Diagnósticos)**.

4. Haga clic en el enlace **View Log (Ver registro)**.

Cómo proteger una máquina

En este tema se describe cómo proteger los datos de una máquina determinada.

NOTA: La máquina debe tener el software de Agent instalado para poder protegerse. Puede instalar el software de Agent antes de realizar este procedimiento, o bien implementarlo en el Agent a medida que configura la protección en el cuadro de diálogo **Connection (Conexión)**. Para conocer los pasos específicos a seguir en la instalación del software de Agent durante el proceso de protección de una máquina, consulte Implementación del sofware de Agent al proteger un Agent.

Cuando agregue protección, debe especificar el nombre o la dirección IP de la máquina a proteger y los volúmenes en esa máquina a proteger, así como definir el programa de protección para cada volumen.

Para proteger varias máquinas a la vez, consulte Protección de varias máquinas.

Para proteger una máquina:

1. Si no lo hizo después de instalar el software de Agent, reinicie la máquina en la que esté instalado el software de Agent.
2. En la Core Console de la máquina del Core, realice una de las siguientes opciones:
   - En la pestaña **Home (Inicio)**, en **Protected Machines (Máquinas protegidas)**, haga clic en **Protect Machine (Proteger máquina)**.
   - Seleccione la pestaña **Machines (Máquinas)** y, en el menú desplegable **Actions (Acciones)**, haga clic en **Protect Machine (Proteger máquina)**.

   Aparecerá el cuadro de diálogo **Connect (Conectar)**.
3. En el cuadro de diálogo **Connect (Conectar)**, introduzca la información sobre la máquina a la que desea conectarse, tal como se describe en la siguiente tabla.

Cuadro de texto	Descripción
Host	El nombre de host o la dirección IP de la máquina que desea proteger.
Port	El número de puerto con el que el Core se comunica con el Agent en la máquina. El número de puerto predeterminado es 8006.
Nombre de usuario	El nombre de usuario que se utiliza para conectarse a ese sistema; por ejemplo, administrador.
Contraseña	La contraseña que se utiliza para conectar a esa máquina.

4. Haga clic en **Connect (Conectar)** para conectar a esa máquina.

   NOTA: Si el software de Agent no está instalado aún en la máquina elegida, siga el procedimiento Implementación del software del Agent al proteger un Agent. Reinicie la máquina del Agent después de implementar el software y continúe con el paso siguiente.
5. En el cuadro de diálogo **Protect (Proteger)**, edite la configuración según sea necesario, tal y como se describe en la tabla siguiente.

Campo	Descripción
Nombre de visualización	Este campo muestra el nombre de host o la dirección IP especificada en el cuadro de diálogo **Connect (Conectar)**. De manera opcional, escriba un nombre nuevo para la máquina que se mostrará en la Core Console. NOTA: También puede cambiar el nombre de visualización más tarde a través de la pestaña **Configuration (Configuración)** de una máquina existente.
Repository (Repositorio)	Seleccione el repositorio en el Core donde se almacenarán los datos de esta máquina.
Encryption Key (Clave de cifrado)	Especifique si el cifrado debe aplicarse a los datos de cada volumen de esta máquina que se almacenarán en el repositorio. NOTA: La configuración del cifrado de un repositorio se define en la pestaña **Configuration (Configuración)** de la Core Console.
Initially Pause Protection (Pausar protección inicialmente)	Después de agregar una máquina para protección, AppAssure comienza a tomar una instantánea base de los datos automáticamente. Puede seleccionar esta casilla de verificación para pausar la protección inicialmente. A continuación, deberá forzar una instantánea manualmente cuando esté listo para iniciar la protección de los datos. Para obtener más información acerca de cómo forzar una instantánea manualmente, consulte Cómo forzar una instantánea.
Volume Groups (Grupos de volúmenes)	Esta opción permite definir los volúmenes que desea proteger y establecer un programa de protección. Para establecer un programa de protección predeterminada cada 60 minutos para todos los volúmenes de la máquina, haga clic en **Apply Default (Aplicar valores predeterminados)**. También puede seleccionar un solo volumen de la máquina y definir sus parámetros de protección de manera individual. Con la configuración inicial, se aplica un programa de protección predeterminado cada 60 minutos. Para modificar el programa para un volumen, haga clic en **Edit (Editar)** en ese volumen. De este modo, podrá definir el intervalo entre instantáneas (además de un programa independiente para los fines de semana) o indicar una hora todos los días en la que se deba tomar la instantánea. Para obtener más información sobre cómo editar el programa de protección de un volumen seleccionado, consulte Creación de programas personalizados para volúmenes.

6. Haga clic en **Protect (Proteger)**.

   La primera vez que se agrega protección para una máquina, se inicia de inmediato la transferencia de una imagen base (una instantánea de todos los datos de los volúmenes protegidos) al repositorio en el Core, salvo que haya especificado pausar la protección inicialmente.

PRECAUCIÓN: Si ha protegido una máquina Linux, no debe desmontar un volumen manualmente. En caso de que necesite hacerlo, ejecute el siguiente comando antes de desmontar el volumen: bsctl -d [path_to_volume]. En este comando, [ruta_del_volumen] no hace referencia al punto de montaje del volumen, sino que se refiere al descriptor de archivo del volumen;debe tener un formato parecido al de este ejemplo: /dev/sda1.

Implementación del software del Agent al proteger un Agent

Puede descargar e implementar Agents cuando está agregando un Agent para protección.

NOTA: Este proceso no es necesario si ya tiene instalado el software del Agent en un sistema que desee proteger.

Para implementar Agents cuando está agregando un Agent para protección:

1. Desde el cuadro de diálogo **Protect Machine (Proteger sistema)** → **Connect (Conectar)**, haga clic en **Connect (Conectar)** después de introducir la configuración de conexión adecuada.

   Se muestra el cuadro de diálogo **Deploy Agent (Implementar Agent)**.
2. Haga clic en **Yes (Sí)** para implementar el software del Agent al sistema de manera remota.

   Se muestra el cuadro de diálogo **Deploy Agent (Implementar Agent)**.
3. Introduzca la configuracion de protección e inicio de sesión de la siguiente manera:
   - **Host name (Nombre de host)**: especifica el nombre de host o dirección IP del sistema que desee proteger.
   - **Port (Puerto)**: especifica el número de puerto con el que el Core se comunica con el Agent del sistema. El valor predeterminado es 8006.
   - **User name (Nombre de usuario)**: especifica el nombre de usuario utilizado para conectarse a este sistema; por ejemplo, administrador.
   - **Password (Contraseña)**: especifica la contraseña utilizada para conectarse a este sistema.
   - **Display name (Nombre para mostrar)**: especifica un nombre para el sistema que se muestra en la Core Console. El nombre para mostrar puede ser el mismo valor que el nombre de host.
   - **Protect machine after install (Proteger máquina después de la instalación)**: al seleccionar esta opción, AppAssure toma una instantánea base de los datos después de agregar la máquina que se va a proteger. Esta opción está seleccionada de manera predeterminada. Si anula la selección de esta opción, deberá forzar una instantánea manual cuando esté listo para iniciar la protección de los datos. Para obtener más información sobre cómo forzar una instantánea manualmente, consulte Cómo forzar una instantánea.
   - **Repository (Repositorio)**: seleccione el repositorio en el que almacenar los datos de este Agent.

     NOTA: Puede almacenar datos de varios Agents en un solo repositorio.
   - **Encryption Key (Clave de cifrado)**: especifica si el cifrado debería aplicarse a los datos para cada volumen de este sistema para almacenarlos en el repositorio.

     NOTA: La configuración del cifrado de un repositorio se define en la ficha **Configuration (Configuración)** de la Core Console.
4. Haga clic en **Deploy (Implementar)**.

   Se cierra el cuadro de diálogo **Deploy Agent (Implementar Agent)**. Puede que haya un retraso antes de que aparezca el Agent seleccionado en la lista de sistemas protegidos.

Creación de programas personalizados para volúmenes

Para crear programas personalizados para volúmenes:

1. En el cuadro de diálogo **Protect Machine (Proteger máquina)** (para obtener información sobre cómo acceder a este cuadro de diálogo, ver la sección Protección de una máquina, en **Volume Groups (Grupos de volúmenes)**, seleccione un volumen para protección y, a continuación, haga clic en **Edit (Editar)**.

   Aparecerá el cuadro de diálogo **Protection Schedule (Programa de protección)**.
2. En el cuadro de diálogo **Protection Schedule (Programa de protección)**, seleccione una de las opciones de programa siguientes para proteger los datos como se describe a continuación:

Cuadro de texto	Descripción
Interval (Intervalo)	Puede elegir entre: • **Weekday (Día de la semana)**:para proteger los datos en un intervalo específico, seleccione **Interval (Intervalo)** y, a continuación: – Para personalizar cuándo se protegen los datos durante las horas de máxima actividad, en los menús desplegables puede especificar una **Start Time (Hora de inicio)**, una **End Time (Hora de finalización)** y un **Interval (Intervalo)**. – Para proteger los datos fuera del horario de máxima actividad, seleccione **Protection interval during off-peak times (Protección fuera del horario de máxima actividad)** y, a continuación, seleccione un intervalo de protección desde el menú desplegable **Time (Hora)**. • **Weekends (Fines de semana)**: para proteger también los datos durante los fines de semana, en el menú desplegable seleccione **Protection interval during weekends (Intervalo de protección durante los fines de semana)** y, a continuación, seleccione un **Interval (Intervalo)**.
Daily (Diariamente)	Para proteger los datos diariamente, seleccione la opción **Daily protection (Protección diaria)** y, a continuación, en el menú desplegable **Time (Hora)** seleccione una hora de inicio de la protección de los datos.
No Protection (Sin protección)	Para eliminar la protección de este volumen, seleccione la opción **No Protection (Sin protección)**.

   Si desea aplicar esa configuración personalizada a todos los volúmenes en esa máquina, seleccione **Apply to All Volumes (Aplicar a todos los volúmenes)**.
3. Cuando haya hecho todos los cambios necesarios, haga clic en **OK (Aceptar)**.
4. Repita el paso 2 y el paso 3 para cualquier volumen adicional que desee personalizar.
5. En el cuadro de diálogo **Protect Machine (Proteger máquina)**, haga clic en **Protect (Proteger)**.

Modificación de la configuración de Exchange Server

Si está protegiendo datos de Microsoft Exchange Server, deberá configurar valores adicionales en la Core Console.

Para modificar la configuración del servidor Exchange:

1. Después de agregar la máquina de Exchange Server para la protección, selecciónela en el panel **Navigation (Navegación)** de la Core Console.

Abrirá la pestaña **Summary (Resumen)** de la máquina.

2. En la pestaña **Summary (Resumen)**, haga clic en el enlace **Exchange Server Settings (Configuración de Exchange Server)**.

   Aparecerá el cuadro de diálogo **Exchange Server Settings (Configuración de Exchange Server)**.

3. En el cuadro de diálogo **Exchange Server Settings (Configuración de Exchange Server)**, puede seleccionar o borrar las configuraciones siguientes:
   - Enable automatic mountability check (Habilitar comprobación de capacidad de montaje automático)
   - Enable nightly checksum check (Habilitar comprobación de suma de comprobación nocturna). Posteriormente, podrá personalizar esta configuración seleccionando una de las siguientes opciones:
     - Automatically truncate Exchange logs after successful checksum check (Truncar automáticamente los registros de Exchange después de una comprobación de suma de comprobación correcta)
     - Truncate log before checksum check completes (Truncar registro antes de que se complete la comprobación de suma de comprobación)
4. También puede modificar las credenciales de inicio de sesión para su Exchange Server. Para ello, deslícese a la sección **Exchange Server Information (Información de Exchange Server)** y, a continuación, haga clic en **Change Credentials (Cambiar credenciales)**.

   Aparecerá el cuadro de diálogo **Set Exchange Credentials (Configurar credenciales de Exchange)**.

5. Introduzca las nuevas credenciales y, a continuación, haga clic en **OK (Aceptar)**.

Modificación de la configuración de SQL Server

Si está protegiendo datos de Microsoft SQL Server, necesitará configurar valores adicionales en la Core Console.

Para modificar la configuración de SQL Server:

1. Después de agregar la máquina de SQL Server para la protección, selecciónela en el panel **Navigation (Navegación)** de la Core Console.

   Abrirá la pestaña **Summary (Resumen)** de la máquina.

2. En la pestaña **Summary (Resumen)**, haga clic en el enlace SQL Server settings (Configuración de SQL Server).

   Se abrirá el cuadro de diálogo **SQL Server Settings (Configuración de SQL Server)**.

3. En el cuadro de diálogo **SQL Server Settings (Configuración de SQL Server)**, edite las configuraciones siguientes, según sea necesario:
   - Enable nightly attachability check (Habilitar comprobación nocturna de conectabilidad)
   - Truncate log after successful attachability check (simple recovery model only) (Truncar el registro tras una comprobación correcta de conectabilidad [solo para el modelo de recuperación simple])
4. También puede modificar las credenciales de inicio de sesión para SQL Server. Para ello, deslícese a la tabla **SQL Server Information (Información de SQLServer)** y, a continuación, haga clic en **Change Credentials (Cambiar credenciales)**.

   Aparecerá el cuadro de diálogo **Set SQL Server Credentials (Configurar credenciales de SQL Server)**.

5. Introduzca las nuevas credenciales y, a continuación, haga clic en **OK (Aceptar)**.

Implementación de un Agent (Instalación de inserción)

AppAssure require microsoft.net para la instalación del Agent. Se debe instalar Microsoft.net en las máquinas del cliente antes de instalar el Agent de forma manual o mediante un proceso de instalación de inserción.

AppAssure le permite implementar el instalador Agent de AppAssure en máquinas Windows individuales para ofrecer protección. Realice los pasos que se indican en el siguiente procedimiento para la instalación automática del instalador en un Agent. Para implementar Agents en varias máquinas simultáneamente, ver Implementación en varias máquinas.

NOTA: Los Agents deben estar configurados con una política de seguridad que permita la instalación remota.

Para implementar un Agent:

1. En la Core Console, haga clic en la pestaña **Machines (Máquinas)**.
2. En el menú desplegable **Actions (Acciones)**, haga clic en **Deploy Agent (Implementar Agent)**.
   Aparecerá el cuadro de diálogo **Deploy Agent (Implementar Agent)**.
3. En el cuadro **Deploy Agent (Implementar Agent)**, introduzca la configuración de inicio de sesión según se indica en la tabla siguiente.

Cuadro de texto	Descripción
Machine (Máquina)	Introduzca el nombre de host o dirección IP de la máquina que quiere implementar.
Nombre de usuario	Introduzca el nombre de usuario con el que conectar a esta máquina (por ejemplo, administrador).
Contraseña	Introduzca la contraseña para conectar a esta máquina.
Automatic reboot after install (Reinicio automático después de la instalación)	Seleccione para especificar si el Core debe iniciarse después de finalizar la implementación e instalación de AppAssure Agent Installer.

4. Haga clic en **Verify (Verificar)** para validar las credenciales que ha introducido.
   El cuadro **Deploy Agent (Implementar Agent)** muestra un mensaje para indicar que la validación se ha realizado.
5. Haga clic en **Abort (Abortar)** si desea cancelar el proceso de verificación.
   Una vez completado el proceso de verificación, aparece un mensaje que indica que la verificación se ha realizado.
6. Haga clic en **Deploy (Implementar)**.
   Se muestra un mensaje que indica que se ha iniciado la implementación. Puede ver el progreso en la pestaña **Events (Eventos)**.
7. Haga clic en **Show details (Mostrar detalles)** para ver más información sobre el estado de la implementación del Agent.
8. Haga clic en **OK (Aceptar)**.

Replicación de un Agent nuevo

Cuando añada un AppAssure Agent para protección en un Core de origen, AppAssure le da la opción de replicar el Agent nuevo en un Core de destino existente.

Para replicar un Agent nuevo:

1. Vaya a la Core Console y seleccione la pestaña **Machines (Máquinas)**.
2. En el menú desplegable **Actions (Acciones)**, haga clic en **Protect Machine (Proteger máquina)**.
3. En el cuadro de diálogo **Protect Machine (Proteger máquina)**, introduzca la información como se describe en la tabla siguiente.

Cuadro de texto	Descripción
Host	Introduzca el nombre de host o la dirección IP de la máquina que desea proteger.
Port (Puerto)	Introduzca el número de puerto por el que el AppAssure Core se comunicará con el Agent en la máquina.
Username (Nombre de usuario)	Introduzca el nombre de usuario que se utiliza para conectar a esa máquina. Por ejemplo, Administrador.
Password (Contraseña)	Introduzca la contraseña que se utiliza para conectarse a esta máquina.

4. Haga clic en **Connect (Conectar)** para conectar a esa máquina.
5. Haga clic en **Show Advanced Options (Mostrar opciones avanzadas)** y edite la configuración siguiente, según sus necesidades.

Cuadro de texto	Descripción
Display Name (Nombre de visualización)	Escriba un nombre para la máquina, que se mostrará en la Core Console.
Repository (Repositorio)	Seleccione el repositorio en el AppAssure Core donde se almacenarán los datos de esta máquina.
Encryption Key (Clave de cifrado)	Especifique si el cifrado debe aplicarse a los datos de cada volumen de esta máquina que se almacenarán en el repositorio. NOTA: La configuración del cifrado de un repositorio se define en la pestaña **Configuration (Configuración)** de la Core Console.
Remote Core (Core remoto)	Especifique el Core de destino en el que desee replicar el Agent.
Remote Repository (Repositorio remoto)	El nombre del repositorio que desee en el Core de destino en el que se almacenarán los datos replicados para esta máquina.
Pause (Pausa)	Marque esta casilla de verificación si desea pausar la replicación; por ejemplo, para pausarla hasta después de que AppAssure tome una imagen base del Agent nuevo.
Schedule (Programa)	Seleccione una de las opciones siguientes: • Protect all volumes with default schedule (Proteger todos los volúmenes con el programa predeterminado)

Cuadro de texto	Descripción
	• Protect specific volumes with custom schedule (Proteger volúmenes específicos con programa personalizado) NOTA: El programa predeterminado es cada 15 minutos.
Initially pause protection (Pausar protección inicialmente)	Seleccione esta casilla de verificación si desea pausar la protección, por ejemplo, para evitar que AppAssure tome una imagen base, hasta que pasen las horas de máxima utilización.

6. Haga clic en **Protect (Proteger)**.

Administración de las máquinas

En esta sección se describen varias tareas que puede realizar para administrar las máquinas, como quitar una máquina del entorno de AppAssure, configurar la replicación, forzar el truncamiento de registro, cancelar operaciones, etc.

Extracción de una máquina

1. Vaya a la Core Console y seleccione la pestaña **Machines (Máquinas)**.
2. En la pestaña **Machines (Máquinas)**, realice una de las acciones siguientes:
   - Haga clic en el hiperenlace de la máquina que desea quitar.
   - O bien, en el panel de navegación, seleccione la máquina que desea quitar.
3. En el menú desplegable **Actions (Acciones)**, haga clic en **Remove Machines (Quitar máquinas)** y, a continuación, seleccione una de las opciones que se describen en la siguiente tabla.

Opción	Descripción
Relationship Only (Sólo relación)	Elimina el Core de origen de la replicación pero mantiene los puntos de recuperación replicados.
With Recovery Points (Con puntos de recuperación)	Elimina el Core de origen de la replicación y elimina todos los puntos de recuperación replicados de dicha máquina.

Replicación de los datos de Agent en una máquina

La replicación es la relación entre los Cores de origen y de destino en el mismo sitio o entre dos sitios con enlace lento por Agent. Si la replicación está configurada entre dos Cores, el Core de origen transmite de forma asíncrona los datos de instantánea incremental de los Agents seleccionados al Core de destino o de origen. La replicación de salida se puede configurar en un proveedor de servicio administrado que proporcione servicio de recuperación de desastres y copia de seguridad externos o en un Core administrado automáticamente. Para replicar datos del Agent en una máquina:

1. En la Core Console, haga clic en la pestaña **Machines (Máquinas)**.
2. Seleccione la máquina que desea replicar.
3. En el menú desplegable **Actions (Acciones)**, haga clic en **Replication (Replicación)** y, a continuación, complete una de las siguientes opciones:

- Si configura la replicación, haga clic en **Enable (Habilitar)**.
- Si ya ha configurado una replicación existente, puede hacer clic en **Copy (Copiar)**.

Aparecerá el cuadro de diálogo **Enable Replications (Habilitar replicación)**.

4. En el cuadro de texto **Host**, introduzca el nombre del host.
5. En **Agents (Agents)**, seleccione la máquina que tiene el Agent y los datos que desea replicar.
6. Si fuera necesario, seleccione la casilla de verificación **Use a seed drive to perform initial transfer (Utilizar una unidad de inicialización para realizar la transferencia inicial)**.
7. Haga clic en **Add (Agregar)**.
8. Para hacer una pausa o para reanudar la replicación, haga clic en **Replication (Replicación)** en el menú desplegable **Actions (Acciones)** y, a continuación, haga clic en **Pause (Pausar)** o en **Resume (Reanudar)** según proceda.

Configuración de la prioridad de replicación para un Agent

Para establecer la prioridad de replicación para un Agent:

1. En la Core Console, seleccione la máquina protegida para la que desee configurar la prioridad de replicación y haga clic en la pestaña **Configuration (Configuración)**.
2. Haga clic en **Select Transfer Settings (Seleccionar configuración de transferencia)** y, a continuación, utilice la lista desplegable **Priority (Prioridad)**, para seleccionar una de las opciones siguientes:
   - **Default (Predeterminado)**
   - **Highest (Más alto)**
   - **Lowest (Más bajo)**
   - **1**
   - **2**
   - **3**
   - **4**

   NOTA: La prioridad predeterminada es 5. Si un Agent recibe la prioridad 1 y otro Agent recibe la prioridad Highest (Más alto), se replica el Agent con prioridad más alta antes que el Agent con prioridad 1.
3. Haga clic en **OK (Aceptar)**.

Cancelación de operaciones en una máquina

Puede cancelar las operaciones actualmente en ejecución de una máquina. Puede especificar cancelar solo una instantánea actual o cancelar todas las operaciones actuales, lo que incluye exportaciones, replicaciones, etc.

Para cancelar las operaciones de una máquina:

1. En la Core Console, haga clic en la pestaña **Machines (Máquinas)**.
2. Seleccione la máquina en la que desea cancelar las operaciones.
3. En el menú desplegable **Actions (Acciones)**, haga clic en **Cancel (Cancelar)** y, a continuación, seleccione una de las siguientes opciones:

Cuadro de texto	Descripción
All Operations (Todas las operaciones)	Cancela todas las operaciones activas para esa máquina.
Snapshot (Instantánea)	Cancela la instantánea actualmente en curso.

Visualización del estado de la máquina y otros detalles

Para ver el estado y otros detalles de la máquina:

1. En el panel de navegación de la Core Console, realice una de las acciones siguientes:
    - Seleccione la pestaña **Machines (Máquinas)** y, a continuación, haga clic en el hiperenlace de la máquina que desea ver.
    - O bien, en el panel de navegación, seleccione la máquina que desea ver.

Aparece la pestaña **Summary (Resumen)**.

La información sobre la máquina se muestra en la página **Summary (Resumen)**. A continuación, se describen los detalles que se incluyen:

- Host Name (Nombre del host)
- Last Snapshot (Última instantánea tomada)
- Next Snapshot (Siguiente instantánea programada)
- Encryption (Estado de cifrado)
- Version number (Número de versión)
- Mountability Check (Estado de comprobación de capacidad de montaje)
- Checksum Check (Estado de comprobación de suma de comprobación)
- Last Log Truncation (Último truncamiento del registro realizado)

También se muestra información sobre los volúmenes contenidos en esta máquina, que incluye:

- Total size (Tamaño total)
- Used Space (Espacio utilizado)
- Free Space (Espacio libre)

Si SQL Server está instalado en la máquina, también se muestra información detallada sobre el servidor, como por ejemplo:

- Nombre
- Install Path (Ruta de instalación)
- Versión
- Número de versión
- Nombre de base de datos
- Estado en línea

Si Exchange Server está instalado en la máquina, también se muestra información detallada sobre el servidor y los almacenes de correo, como por ejemplo:

- Nombre

- Install Path (Ruta de instalación)
- Data Path (Ruta de acceso datos)
- Name Exchange Databases Path (Poner nombre a ruta de acceso a bases de datos de Exchange)
- Log File Path (Ruta de acceso al archivo de registro)
- Log Prefix (Prefijo de registro)
- System Path (Ruta de acceso al sistema)
- MailStore Type (Tipo de almacén de correo)

Administración de varias máquinas

En este tema se describen las tareas que los administradores deben realizar para implementar el software de Agent de forma simultánea en varias máquinas Windows.

Para implementar y proteger varios Agents, debe realizar las tareas siguientes:

1. Implementar AppAssure en varias máquinas.
   Consulte Implementación en varias máquinas.
2. Supervisar la actividad de la implementación por lotes.
   Consulte Supervisión de la implementación de varias máquinas.
3. Proteger varias máquinas.
   Consulte Protección de varias máquinas.

   NOTA: Este paso puede omitirse si seleccionó la opción Protect machine after install (Proteger la máquina después de la instalación) durante la implementación.
4. Supervisar la actividad de la protección por lotes.
   Consulte Supervisión de la protección de varias máquinas.

Implementación en varias máquinas

Puede simplificar la tarea de implementación del software AppAssure Agent en varias máquinas Windows mediante la función Bulk Deploy (Implementación masiva) de AppAssure. Puede realizar la Implementación masiva en:

- Máquinas en un host virtual VMware vCenter/ESXi
- Máquinas en un dominio de Active Directory
- Máquinas en cualquier otro host

La función Bulk Deploy (Implementación masiva) detecta automáticamente máquinas en un host y le permite seleccionar aquellas en las que desee realizar la implementación. De manera alternativa, puede introducir manualmente información del host y la máquina.

NOTA: Las máquinas que va a implementar deben tener acceso a Internet para poder descargar e instalar bits, ya que AppAssure usa la versión web del instalador de AppAssure Agent para implementar los componentes de la instalación. Si no dispone de conexión a Internet, puede ejecutar el programa de instalación de AppAssure Agent desde la máquina del Core. Para obtener más información acerca de cómo ejecutar la instalación del Agent desde la máquina del Core, consulte Ejecución del Programa de instalación del Agent desde la máquina del Core. También puede descargar actualizaciones del Core y del Agent desde el Portal de licencias.

Inserción del programa de instalación del Agent desde la máquina del Core

Si los servidores que se van a implementar no tienen acceso a Internet, puede insertar el archivo de instalación del Agent actual desde la máquina del Core. El appliance DL4000 incluye el archivo del programa de instalación del Agent.

NOTA: Descargue las actualizaciones del Core y del Agent del Portal de licencias.

Para insertar el programa de instalación del Agent desde la máquina del Core:

1. En la máquina del Core, copie el archivo de instalación del Agent **Agent-X64–5.x.x.xxxxx.exe** en el directorio **C:\Program Files\apprecovery\core\installers**.
2. En la Core Console, seleccione la pestaña **Configuration (Configuración)** y, a continuación, haga clic en **Settings (Valores)**.
3. En la sección **Deploy Settings (Implementar configuración)**, edite el **Agent Installer Name (Nombre del instalador del Agent)**.

Implementación en máquinas en un dominio de Active Directory

Antes de iniciar este procedimiento, debe tener la información de dominio y las credenciales de inicio de sesión para el servidor de Active Directory.

Para implementar el Agent en varias máquinas en un dominio de Active Directory:

1. En la Core Console, haga clic en la pestaña **Tools (Herramientas)** y, a continuación, en **Bulk Deploy (Implementación masiva)**.
2. En la ventana **Deploy Agent to Machines (Implementar Agent en máquinas)**, haga clic en **Active Directory**.
3. En el cuadro de diálogo **Connect to Active Directory (Conectar con Active Directory)**, introduzca la información del dominio y las credenciales de inicio de sesión de la siguiente tabla:

Cuadro de texto	Descripción
Dominio	El nombre de host o la dirección IP del dominio de Active Directory.
Nombre de usuario	El nombre de usuario que se utiliza para conectarse al dominio (por ejemplo, Administrador).
Contraseña	La contraseña segura que se utiliza para conectase al dominio.

4. Haga clic en **Connect (Conectar)**.
5. En el cuadro de diálogo **Add Machines from Active Directory (Agregar máquinas desde Active Directory)**, seleccione las máquinas en las que desea implementar AppAssure Agent y, continuación, haga clic en **Add (Agregar)**.

   Las máquinas agregadas aparecen en la ventana **Deploy Agent on Machines (Implementar Agent en máquinas)**.
6. Para introducir la contraseña de la máquina, seleccione un repositorio, agregue una clave de cifrado o edite otra configuración de la máquina, haga clic en el enlace **Edit (Editar)** de esa máquina y, a continuación, realice los siguientes pasos.
   a. En el cuadro de diálogo **Edit Settings (Editar configuración)**, introduzca la información que se describe en la tabla siguiente.

Cuadro de texto	Descripción
Host Name (Nombre del host)	Se proporciona automáticamente desde el paso 3.
Nombre de visualización	Se asigna automáticamente en función del nombre de host especificado en el paso 3.
Port	El número de puerto por el que el Core se comunica con el Agent en la máquina.
Nombre de usuario	Se proporciona automáticamente desde el paso 3.
Contraseña	Introduzca la contraseña de la máquina.
Automatic reboot after install (Reinicio automático después de la instalación)	Especifique si desea iniciar automáticamente la máquina tras la implementación. NOTA: Esta opción es obligatoria si desea proteger automáticamente la máquina tras la implementación activando la casilla **Protect Machine After Install (Proteger máquina tras la instalación)**.
Protect Machine After Install (Proteger máquina tras la instalación)	Especifique si desea proteger automáticamente la máquina tras la implementación. Esto le permitirá omitir **Protecting Multiple Machines (Protección de varias máquinas)**.
Repository (Repositorio)	En la lista desplegable, seleccione el repositorio de Core en el que desea almacenar los datos de las máquinas. El repositorio que seleccione se utilizará para todas las máquinas que se vayan a proteger. NOTA: Esta opción solo está disponible al seleccionar **Protect machine after install (Proteger máquina tras la instalación)**.
Encryption Key (Clave de cifrado)	(Opcional) Use la lista desplegable para especificar si se debe aplicar cifrado a los datos de las máquinas que se almacenen en el repositorio. La clave de cifrado se asigna a todas las máquinas que se vayan a proteger. NOTA: Esta opción solo está disponible al seleccionar **Protect machine after install (Proteger máquina tras la instalación)**.

b. Haga clic en **Save (Guardar)**.

7. Para comprobar si AppAssure se conecta a las máquinas correctamente, seleccione cada una de las máquinas en la ventana **Deploy Agent on Machines (Implementar Agent en máquinas)** y haga clic en **Verify (Verificar)**.
8. La ventana **Deploy Agent on Machines (Implementar Agent en máquinas)** muestra un icono junto a cada máquina que refleja su preparación para la implementación, como se indica a continuación:

Cuadro de texto	Descripción
Icono verde	AppAssure se puede conectar a la máquina y está listo para su implementación.
Icono amarillo	AppAssure se puede conectar a la máquina; sin embargo, el Agent está ya emparejado con una máquina del Core.

Cuadro de texto	Descripción
Icono rojo	AppAssure no se puede conectar a la máquina. Esto puede deberse a que las credenciales de inicio de sesión sean incorrectas, la máquina esté apagada, el servidor de seguridad esté bloqueando el tráfico u otro problema. Para corregirlo, haga clic en **Edit Settings (Editar configuración)** en la barra de herramientas o en el enlace **Edit (Editar)** situado junto a la máquina.

9. Después de comprobar las máquinas correctamente, seleccione aquellas en las que desea implementar AppAssure Agent y, continuación, haga clic en **Deploy (Implementar)**.
10. Si ha seleccionado la opción **Protect machine after install (Proteger máquina tras la instalación)**, una vez que la implementación sea satisfactoria, las máquinas se inician automáticamente y se habilita la protección.

Implementación a máquinas en un host virtual VMware vCenter o ESXi

Antes de iniciar este procedimiento, debe tener la información de ubicación del host y credenciales de inicio de sesión para el host virtual VMware vCenter/ESXi.

NOTA: Todas las máquinas virtuales deben tener VM Tools (Herramientas de VM) instaladas; de lo contrario, AppAssure no puede detectar el nombre del host de la máquina virtual a la que implementar. En lugar del nombre del host. AppAssure usa el nombre de máquina virtual, lo que puede provocar problemas si el nombre del host no coincide con el nombre de la máquina virtual.

Para implementar en múltiples máquinas en un host virtual vCenter/ESXi:

1. En la Core Console, haga clic en la pestaña **Tools (Herramientas)** y, a continuación, en **Bulk Deploy (Implementación masiva)**.
2. En la ventana **Deploy Agent on Machines (Implementar Agent en máquinas)**, haga clic en **vCenter/ESXi**.
3. En el cuadro de diálogo **Connect to VMware vCenter Server/ESXi (Conectar a VMware vCenter Server/ESXi)**, introduzca la información del host y credenciales de inicio de sesión como se indica a continuación y haga clic en **OK (Aceptar)**.

Cuadro de texto	Descripción
Host	Escriba el nombre o la dirección IP del host virtual de VMware vCenter Server/ESX(i).
User Name (Nombre de usuario)	Escriba el nombre de usuario con el que conectar al host virtual; por ejemplo, administrador.
Contraseña	Introduzca la contraseña segura que se utiliza para conectarse al host virtual.

4. En el cuadro de diálogo **Add Machines from VMware vCenter Server/ESXi (Agregar máquinas desde VMware vCenter Server/ESXi)**, seleccione la casilla situada junto a las máquinas en las que desea implementar el AppAssure Agent y, a continuación, haga clic en **Add (Agregar)**.
5. En la ventana **Deploy Agent on Machines (Implementar Agent en máquinas)**, puede ver las máquinas que ha agregado. Si desea seleccionar un repositorio, clave de cifrado u otra configuración para una máquina, seleccione el cuadro de verificación situado junto a la máquina y haga clic en **Edit Settings (Editar configuración)**.

   Para obtener más detalles sobre cada configuración, consulte Implementación en máquinas en un dominio de Active Directory.

6. Compruebe si AppAssure se conecta a las máquinas correctamente. Seleccione cada una de las máquinas en la ventana **Deploy Agent on Machines (Implementar Agent en máquinas)** y, a continuación, haga clic en **Verify (Verificar)**.
7. La ventana **Deploy Agent on Machines (Implementar Agent en máquinas)** muestra un icono junto a cada máquina que refleja su preparación para la implementación, como se indica a continuación:

Cuadro de texto	Descripción
Icono verde	AppAssure se puede conectar a la máquina y está listo para su implementación.
Icono amarillo	AppAssure se puede conectar a la máquina; sin embargo, el Agent está ya emparejado con una máquina del Core.
Icono rojo	AppAssure no se puede conectar a la máquina. Esto puede deberse a que las credenciales de inicio de sesión sean incorrectas, la máquina esté apagada, el servidor de seguridad esté bloqueando el tráfico u otro problema. Para corregirlo, haga clic en **Edit Settings (Editar configuración)** en la barra de herramientas o en el enlace **Edit (Editar)** situado junto a la máquina.

8. Después de verificar las máquinas correctamente, seleccione cada una de ellas y haga clic en **Deploy (Implementar)**.
9. Si ha seleccionado la opción **Protect machine after install (Proteger máquina tras la instalación)**, una vez la implementación sea satisfactoria, las máquinas se reiniciarán automáticamente y se habilitará la protección.

Implementación en máquinas en cualquier otro host

Para implementar en máquinas en cualquier otro host:

1. En la Core Console, haga clic en la pestaña **Tools (Herramientas)** y, a continuación, en **Bulk Deploy (Implementación masiva)**.
2. En la ventana **Deploy Agent on Machines (Implementar Agent en máquinas)**, realice una de las acciones siguientes:
   - Haga clic en **New (Nuevo)** para especificar varias máquinas mediante el cuadro de diálogo **Add Machine (Agregar máquina)**; esto le permite introducir un nuevo host de máquina, credenciales de inicio de sesión, repositorio, clave de cifrado e información adicional. Para obtener detalles sobre cada valor, ver Implementación en máquinas en un dominio de Active Directory.

     Después de introducir esta información, haga clic en **OK (Aceptar)** para agregarla a la lista **Deploy Agent on Machines (Implementar Agent en máquinas)**, o haga clic en **OK & New (Aceptar y Nuevo)** para agregar otra máquina.

     NOTA: Si desea proteger la máquina automáticamente después de la implementación, seleccione la casilla de verificación **Protect Machine after Install (Proteger máquina tras instalación)**. Si marca la casilla de verificación, la máquina se reinicializa automáticamente antes de habilitar la protección.
   - Haga clic en **Manually (Manualmente)** para especificar varias máquinas en una lista; cada línea representa una máquina para implementar. En el cuadro de diálogo **Add Machines Manually (Agregar máquinas manualmente)**, introduzca la dirección IP o el nombre de la máquina, el nombre de usuario, la contraseña, separados por un delimitador doble de dos puntos y el puerto, como se indica a continuación:

     ```
     hostname::username::password::port For example:
     10.255.255.255::administrator::&11@yYz90z::8006 abc-
     host-00-1::administrator::99!zU$o83r::168
     ```
3. En la ventana **Deploy Agent on Machines (Implementar Agent en máquinas)**, puede ver las máquinas que ha agregado. Si desea seleccionar un repositorio, clave de cifrado u otra configuración

para una máquina, seleccione el cuadro de verificación situado junto a la máquina y haga clic en **Edit Settings (Editar configuración)**.

Para obtener más detalles sobre cada configuración, consulte Implementación en máquinas en un dominio de Active Directory.

4. Compruebe si AppAssure se conecta a las máquinas correctamente. Seleccione cada una de las máquinas en la ventana **Deploy Agent on Machines (Implementar Agent en máquinas)** y, a continuación, haga clic en **Verify (Verificar)**.

   La ventana **Deploy Agent on Machines (Implementar Agent en máquinas)** muestra un icono junto a cada máquina que refleja su preparación para la implementación, como se indica a continuación:

Cuadro de texto	Descripción
Icono verde	AppAssure se puede conectar a la máquina y está listo para su implementación.
Icono amarillo	AppAssure se puede conectar a la máquina; sin embargo, el Agent está ya emparejado con una máquina del Core.
Icono rojo	AppAssure no se puede conectar a la máquina. Esto puede deberse a que las credenciales de inicio de sesión sean incorrectas, la máquina esté apagada, el servidor de seguridad esté bloqueando el tráfico u otro problema. Para corregirlo, haga clic en **Edit Settings (Editar configuración)** en la barra de herramientas o en el enlace **Edit (Editar)** situado junto a la máquina.

5. Una vez se hayan verificado las máquinas correctamente, marque la casilla junto a cada máquina y haga clic en **Deploy (Implementar)**.
6. Si ha seleccionado la opción **Protect machine after install (Proteger máquina tras la instalación)**, una vez la implementación sea satisfactoria, las máquinas se reiniciarán automáticamente y se habilitará la protección.

Supervisión de la implementación de varias máquinas

Puede ver el progreso de la implementación del software AppAssure Agent en las máquinas.

Para supervisar la implementación en varias máquinas:

1. En la Core Console, haga clic en la pestaña **Events (Eventos)**, busque la tarea de implementación en la lista y haga clic en el botón de la columna **Details (Detalles)**.

   La ventana **Monitor Active Task (Supervisar tarea activa)** muestra los detalles de la implementación.

   Incluye información global del progreso, así como el estado de cada implementación individual. Aparecen los siguientes detalles:

   - Hora de inicio
   - Hora de finalización
   - Tiempo transcurrido
   - Tiempo restante
   - Progreso
   - Fase
2. Realice uno de los siguientes pasos:
   - Haga clic en **Open in New window (Abrir en una ventana nueva)** para iniciar una nueva ventana para ver el progreso de la implementación.
   - Haga clic en **Close (Cerrar)** y las tareas de implementación se procesarán en segundo plano.

Protección de varias máquinas

Tras la implementación masiva del software de Agent en las máquinas de Windows, debemos ahora protegerlas para proteger los datos. Si selecciona **Protect Machine After Install (Proteger máquina tras la instalación)** al implementar el Agent, podrá saltarse este procedimiento.

NOTA: Las máquinas de Agent se deben configurar con una política de seguridad que permita que la instalación remota sea posible.

Para proteger varias máquinas:

1. En la Core Console, haga clic en la pestaña **Tools (Herramientas)** y, a continuación, haga clic en **Bulk Protect (Protección masiva)**.

   Aparecerá la ventana **Protect Machines (Proteger máquinas)**.
2. Agregue las máquinas que desea proteger haciendo clic en una de las siguientes opciones.

   Para obtener detalles sobre cómo completar cada opción, consulte Implementación en varias máquinas.

   - Haga clic en **Active Directory** para especificar máquinas en un dominio de Active Directory.
   - Haga clic en **vCenter/ESXi** para especificar máquinas virtuales en un host virtual vCenter/ESXi.
   - Haga clic en **New (Nuevo)** para especificar varias máquinas utilizando el cuadro de diálogo Add Machine (Agregar máquina).
   - Haga clic en **Manually (Manualmente)** para especificar varias máquinas en una lista escribiendo el nombre de host y las credenciales.
3. En la ventana **Protect Machines (Proteger máquinas)**, puede ver las máquinas que ha agregado. Si desea seleccionar un repositorio, una clave de cifrado u otra configuración avanzada para una máquina, active la casilla situada junto a la máquina y haga clic en **Edit Settings (Editar configuración)**.
4. Especifique la configuración como se indica a continuación y haga clic en **OK (Aceptar)**.

Cuadro de texto	Descripción
Nombre de usuario	Introduzca el nombre de usuario que se utiliza para conectar a esa máquina; por ejemplo, Administrador.
Contraseña	Introduzca la contraseña segura que se utiliza para conectarse a esta máquina.
Port	Especifique el número de puerto por el que el Core se comunica con el Agent en la máquina.
Repository (Repositorio)	Seleccione el repositorio del Core en el que se almacenan los datos de las máquinas. El repositorio que seleccione se utilizará para todas las máquinas que se vayan a proteger.
Encryption Key (Clave de cifrado)	Especifique si se aplica cifrado al Agent de las máquinas que se almacena en el repositorio. La clave de cifrado se asigna a todas las máquinas que se vayan a proteger.
Protection Schedule (Programa de protección)	Indique el programa para el que se produce la protección de la máquina. El programa predeterminado es 60 minutos durante las horas punta de funcionamiento y 60 minutos los fines de semana. Para editar el programa para adaptarlo a las necesidades de su empresa, haga clic en **Edit (Editar)**.

Cuadro de texto	Descripción
	NOTA: Para obtener más información, consulte Modificación de los programas de protección.
Initially Pause Protection (Pausar protección inicialmente)	De manera opcional, puede elegir pausar la protección durante la primera ejecución;es decir, el Core no realizará instantáneas de las máquinas hasta que reanude manualmente la protección.

5. Verifique que AppAssure se puede conectar a cada máquina correctamente. Para ello, active la casilla situada junto a cada máquina en la ventana **Protect Machines (Proteger máquinas)** y haga clic en **Verify (Verificar)**.
6. La ventana **Protect Machines (Proteger máquinas)** muestra un icono junto a cada máquina que refleja su preparación para la implementación, de la siguiente forma:

Icono	Descripción
Icono verde	AppAssure se puede conectar a la máquina y está listo para su protección.
Icono amarillo	AppAssure se puede conectar a la máquina; sin embargo, el Agent está ya emparejado con una máquina del Core.
Icono rojo	AppAssure no se puede conectar a la máquina. Esto puede deberse a que las credenciales de inicio de sesión sean incorrectas, la máquina esté apagada, el servidor de seguridad esté bloqueando el tráfico u otro problema. Para corregirlo, haga clic en **Edit Settings (Editar configuración)** en la barra de herramientas o en el enlace **Edit (Editar)** situado junto a la máquina.

7. Una vez se hayan verificado las máquinas correctamente, active la casilla junto a cada máquina y haga clic en **Protect (Proteger)**.

Supervisión de la protección de varias máquinas

Puede supervisar el progreso a medida que AppAssure aplica las políticas y programas de protección a las máquinas.

Para supervisar la protección de varias máquinas:

1. Haga clic en la pestaña **Machines (Máquinas)** para ver el estado y el progreso de la protección.
   Aparecerá la página **Protected Machines (Máquinas protegidas)**.
2. Seleccione la pestaña **Events (Eventos)** para ver las tareas, eventos y alertas relacionados.
   Aparecerá la página **Tasks (Tareas)** .

Cuadro de texto	Descripción
Para ver información de tarea	A medida que los volúmenes se transfieren, el estado, las horas de inicio y las horas de finalización aparecen en el panel **Tasks (Tareas)**. Haga clic en **Details (Detalles)** para ver información más específica sobre la tarea.
Para ver información de alerta	A medida que se agrega cada máquina protegida, se registra una alerta que detalla si la operación ha sido satisfactoria o si se han registrado errores. Aparece el nivel de la alerta junto con la fecha y el mensaje transaccional. Si desea quitar todas las alertas de la página, haga clic en **Dismiss All (Descartar todo)**.

Cuadro de texto	Descripción
Para ver información de evento	Los detalles sobre la máquina y los datos que se transfieren se muestran en el panel **Events(Eventos)**. Aparecen el nivel del evento, la fecha transaccional y el mensaje de tiempo.

Administración de instantáneas y puntos de recuperación

Un punto de recuperación es una colección de instantáneas tomadas de volúmenes de disco independientes que se almacenan en el repositorio. Las instantáneas capturan y almacenan el estado de un volumen de disco en un punto específico en el tiempo mientras las aplicaciones que generan los datos aún están en uso. En AppAssure, puede forzar instantáneas, pausar instantáneas de manera temporal o ver listas de los puntos de recuperación actuales en el repositorio, así como eliminarlos si es necesario. Los puntos de recuperación se usan para restaurar las máquinas protegidas o montar máquinas en un sistema de archivos local.

Las instantáneas que AppAssure captura se capturan a nivel de bloque y son sensibles a las aplicaciones. Esto implica que se completen todas las transacciones abiertas y registros de transacciones en movimiento y que las cachés se despejen a disco antes de crear la instantánea.

AppAssure utiliza un controlador de filtro de volumen de bajo nivel que se conecta a los volúmenes montados y, a continuación, realiza el seguimiento de todos los cambios a nivel de bloque para la siguiente instantánea inminente. Se utiliza Microsoft Volume Shadow Services (VSS) para facilitar instantáneas consistentes de bloqueo de aplicación.

Visualización de puntos de recuperación

Para ver los puntos de recuperación:

1. En el área de navegación izquierda de la Core Console, seleccione la máquina para la que desea ver los puntos de recuperación y, a continuación, haga clic en la ficha **Recovery Points (Puntos de recuperación)**.

Puede ver la información sobre los puntos de recuperación de la máquina según se describe en la tabla siguiente:

Informativa	Descripción
Estado	Indica el estado actual del punto de recuperación.
Cifrados	Indica si el punto de recuperación está cifrado.
Content (Contenido)	Muestra los volúmenes incluidos en el punto de recuperación.
Tipo	Define un tipo de punto de recuperación, básico o diferencial.
Creation Date (Fecha de creación)	Muestra la fecha de creación del punto de recuperación.
Tamaño	Muestra la cantidad de espacio que el punto de recuperación consume en el repositorio.

Visualización de un punto de recuperación específico

Para ver un punto de recuperación específico:

1. En el área de navegación izquierda de la Core Console, seleccione la máquina para la que desea ver los puntos de recuperación y, a continuación, haga clic en la pestaña **Recovery Points (Puntos de recuperación)**.
2. Haga clic en el símbolo **>** junto a un punto de recuperación de la lista para expandir la vista.

   Podrá ver información más detallada acerca del contenido del punto de recuperación para la máquina seleccionada, además de acceder a diversas operaciones que se pueden ejecutar en el punto de recuperación, y que se enumeran en la siguiente tabla:

Informativa	Descripción
Acciones	En el menú **Actions (Acciones)** se incluyen las siguientes operaciones que se pueden ejecutar en el punto de recuperación seleccionado: **Mount (Montar)**: seleccione esta opción para montar el punto de recuperación seleccionado. Para obtener más información acerca de cómo montar un punto de recuperación seleccionado, consulte Montaje de un punto de recuperación para una máquina Windows. **Export (Exportar)**: esta opción permite exportar el punto de recuperación seleccionado a ESXi, a una estación de trabajo VMware o a HyperV. Para obtener más información acerca de cómo exportar puntos de recuperación, consulte Exportación de información de copia de seguridad de su máquina Windows a una máquina virtual. **Rollback (Revertir)**: seleccione esta opción para restaurar desde el punto de recuperación seleccionado al volumen que especifique. Para obtener más información acerca de cómo restaurar desde puntos de recuperación seleccionados, consulte Cómo iniciar una restauración desde AppAssure Core.

3. Haga clic en el símbolo **>** junto a un volumen en el punto de recuperación seleccionado para expandir la vista.

Puede ver la información sobre el volumen seleccionado en el punto de recuperación expandido según se describe en la tabla siguiente:

Cuadro de texto	Descripción
Título	Muestra el volumen específico del punto de recuperación.
Capacidad nativa	Indica la cantidad de espacio de almacenamiento libre en el volumen.
Capacidad con formato	Indica la cantidad de espacio de almacenamiento disponible para los datos una vez que el volumen se ha formateado.
Capacidad usada	Indica la cantidad de espacio de almacenamiento utilizada actualmente en el volumen.

Montaje de un punto de recuperación para una máquina Windows

En AppAssure puede montar un punto de recuperación para una máquina Windows para acceder a los datos almacenados a través de un sistema de archivos local.

Para montar un punto de recuperación para una máquina Windows:

1. En la Core Console, realice una de las acciones siguientes:
   - Seleccione la pestaña **Machines (Máquinas)**.

     a. Al lado de la máquina o clúster con el punto de recuperación que desee montar, seleccione **Mount (Montar)** en el menú desplegable **Actions (Acciones)**.
     b. Seleccione un punto de recuperación en la lista en el cuadro de diálogo **Mount Recovery Point (Montar punto de recuperación)** y, a continuación, haga clic en **Next (Siguiente)**.

     Aparecerá el cuadro de diálogo **Mount Recovery Point (Montar punto de recuperación)**.
   - En la Core Console, elija la máquina que desea montar en un sistema de archivos local.

     Aparece la pestaña **Summary (Resumen)** para la máquina seleccionada.

     a. Seleccione la pestaña **Recovery Points (Puntos de recuperación)**.
     b. En la lista de puntos de recuperación, expanda el punto de recuperación que desea montar.
     c. En los detalles expandidos de ese punto de recuperación, haga clic en **Mount (Montar)**.

     Aparecerá el cuadro de diálogo **Mount Recovery Point (Montar punto de recuperación)**.
2. En el cuadro de diálogo **Mount (Montar)**, edite los cuadros de texto para montar un punto de recuperación como se describe en la tabla siguiente:

Cuadro de texto	Descripción
Mount Location: Local Folder (Ubicación de montaje: carpeta local)	Especifica la ruta de acceso que se utiliza para acceder al punto de recuperación montado.
Volume Images (Imágenes de volumen)	Especifica las imágenes de volumen que desea montar.
Mount Type (Tipo de montaje)	Especifica la forma para acceder a los datos para el punto de recuperación montado. • Mount Read-only (Montaje de solo lectura). • Mount Read-only with previous writes (Montaje de solo lectura con escrituras previas). • Mount Writable (Montaje con capacidad de escritura).
Create a Windows share for this Mount (Crear un recurso compartido de	Opcionalmente, seleccione la casilla de verificación para especificar si el punto de recuperación montado se puede compartir y, en ese caso, configurar los derechos de acceso, incluidos el nombre del recurso compartido y los grupos de acceso.

Cuadro de texto	Descripción
Windows para este montaje)	

3. Haga clic en **Mount (Montar)** para montar el punto de recuperación.

Desmontaje de puntos de recuperación seleccionados

Puede desmontar algunos puntos de recuperación que se montan localmente en el Core.

Para desmontar puntos de recuperación seleccionados:

1. En la Core Console, seleccione la pestaña **Tools (Herramientas)**.
2. En la opción **Tools (Herramientas)**, haga clic en **System Info (Información del sistema)**.
3. Busque y seleccione la disposición del montaje del punto de recuperación que desea desmontar y, a continuación, haga clic en **Dismount (Desmontar)**.

Desmontaje de todos los puntos de recuperación

Puede desmontar todos los puntos de recuperación que se montan localmente en el Core.

Para desmontar todos los puntos de recuperación:

1. En la Core Console, seleccione la pestaña **Tools (Herramientas)**.
2. En la opción **Tools (Herramientas)**, haga clic en **System Info (Información del sistema)**.
3. En la sección **Local Mounts (Montajes locales)**, haga clic en **Dismount All (Desmontar todo)**.

Montaje de un volumen de punto de recuperación en una máquina Linux

1. Cree un nuevo directorio para montar el punto de recuperación (por ejemplo, puede usar el comando `mkdir`).
2. Verifique que el directorio existe (por ejemplo, mediante el comando `ls`).
3. Ejecute la utilidad **aamount** de AppAssure como raíz o como el superusuario, por ejemplo:

   ```
   sudo aamount
   ```

4. En la solicitud de montaje de AppAssure, introduzca el siguiente comando para enumerar las máquinas protegidas.

   ```
   lm
   ```

5. Cuando se le solicite, introduzca la dirección IP o nombre del host del servido AppAssure Core.
6. Introduzca las credenciales de inicio de sesión para el servidor del Core, es decir, el nombre de usuario y la contraseña.

   Se muestra una lista que muestra las máquinas protegidas por este servidor AppAssure. Enumera las máquinas encontradas por número de elemento de línea, dirección de host/IP y un número de Id. para la máquina (por ejemplo: `293cc667-44b4-48ab-91d8-44bc74252a4f`).
7. Introduzca el siguiente comando para enumerar los puntos de recuperación montados actualmente para una máquina especificada:

   ```
   lr <line_number_of_machine>
   ```

   NOTA: También puede introducir el número de Id. de la máquina en lugar del número de elemento de línea.

Se muestra una lista que muestra los puntos de recuperación base e incrementales para esa máquina. Esta lista incluye un número de elemento de línea, fecha/fecha y hora, ubicación del volumen y un número de Id. para el volumen que incluye un número de secuencia al final (por ejemplo, `293cc667-44b4-48ab-91d8-44bc74252a4f:2`), que identifica el punto de recuperación.

8. Introduzca el siguiente comando para seleccionar y montar el punto de recuperación especificado en el punto/ruta de acceso de montaje especificados.

   `m <volume_recovery_point_ID_number> <path>`

   NOTA: También puede especificar un número de línea en el comando en lugar del número de Id. del punto de recuperación. En este caso, utilice el número de línea del Agent o de la máquina (desde la salida lm), seguido por el número de línea del punto de recuperación y la letra del volumen, y a continuación la ruta de acceso, como por ejemplo, `m <machine_line_number> <recovery_point_line_number> <volume_letter> <path>`. Por ejemplo, si la salida `lm` enumera tres máquinas Agent, e introduce el comando `lr` para el número 2 y monta el volumen b del punto de recuperación 23 para **/tmp/mount_dir** el comando es: `m 2 23 b /tmp/mount_dir`.

   PRECAUCIÓN: No debe desmontar un volumen de Linux protegido manualmente. En caso de que necesite hacerlo, debe ejecutar el siguiente comando antes de desmontar el volumen: `bsctl -d <path to volume>`. En este comando, `<path to volume>` no se hace referencia al punto de montaje del volumen, sino al descriptor de archivo del volumen; debe tener un formato similar a este ejemplo: /dev/sda1.

Eliminación de puntos de recuperación

Puede fácilmente eliminar puntos de recuperación de una máquina específica desde el repositorio.Al eliminar puntos de recuperación en AppAssure, puede especificar una de las siguientes opciones:

Cuadro de texto	Descripción
Delete All Recovery Points (Eliminar todos los puntos de recuperación)	Elimina todos los puntos de recuperación para la máquina Agent seleccionada del repositorio.
Delete a Range of Recovery Points (Eliminar un rango de puntos de recuperación)	Elimina todos los puntos de recuperación de un rango especificado antes del actual, hasta e incluida la imagen base, que son todos los datos de la máquina, así como todos los puntos de recuperación después del actual hasta la imagen base siguiente.

NOTA: No podrá recuperar los puntos de recuperación que haya eliminado.

Para eliminar puntos de recuperación:

1. En el área de navegación izquierda de la Core Console, seleccione la máquina para la que desea ver los puntos de recuperación y, a continuación, haga clic en la ficha **Recovery Points (Puntos de recuperación)**.
2. Haga clic en el menú **Actions (Acciones)**.
3. Seleccione una de las opciones siguientes:
   - Para eliminar todos los puntos de recuperación actualmente almacenados, haga clic en **Delete All (Eliminar todos)**.
   - Para eliminar un conjunto de puntos de recuperación en un rango de datos específico, haga clic en **Delete Range (Eliminar rango)**. Se muestra el cuadro de diálogo **Delete (Eliminar)**. En el cuadro de diálogo **Delete Range (Eliminar rango)**, especifique el rango de puntos de

recuperación que desea eliminar utilizando una fecha y hora de inicio y una fecha y hora de finalización;a continuación, haga clic en **Delete (Eliminar)**.

Eliminación de una cadena de puntos de recuperación huérfanos

Un punto de recuperación huérfano es una instantánea incremental que no está asociada a ninguna imagen base. Las instantáneas posteriores siguen creándose en este punto de recuperación. Sin la imagen base, los puntos de recuperación que se originan están incompletos y es poco probable que contengan los datos necesarios para realizar una recuperación. Se considera que estos puntos de recuperación forman parte de la cadena de puntos de recuperación huérfanos. En caso de producirse esta situación, la mejor solución consiste en eliminar la cadena y crear una imagen base nueva.

NOTA: La capacidad para eliminar una cadena de puntos de recuperación huérfanos no está disponible para los puntos de recuperación replicados en un Core de destino.

Para eliminar una cadena de puntos de recuperación huérfanos:

1. En la Core Console, seleccione la máquina protegida para la que desea eliminar la cadena de puntos de recuperación huérfanos.
2. Haga clic en la pestaña **Recovery Points (Puntos de recuperación)**.
3. En **Recovery Points (Puntos de recuperación)**, expanda el punto de recuperación huérfano.

   En la columna **Type (Tipo)**, este punto de recuperación aparece como **Incremental Orphaned (Huérfano incremental)**.
4. Junto a **Actions (Acciones)**, haga clic en **Delete (Eliminar)**.

   Aparece la ventana **Delete Recovery Points (Eliminar puntos de recuperación)**.
5. En la ventana **Delete Recovery Points (Eliminar puntos de recuperación)**, haga clic en **Yes (Sí)**.

   PRECAUCIÓN: Al eliminar este punto de recuperación se elimina toda la cadena de puntos de recuperación, incluidos los puntos incrementales situados antes o después de la cadena, hasta la imagen base siguiente. Esta operación no se puede deshacer.

   La cadena de puntos de recuperación huérfanos se elimina.

Cómo forzar una instantánea

Forzar una instantánea le permite forzar una transferencia de datos para la máquina protegida actual. Cuando se fuerza una instantánea, la transferencia se inicia inmediatamente o se agrega a la cola. Solo se transfieren los datos que hayan cambiado desde un punto de recuperación anterior. Si no existe ningún punto de recuperación anterior, se transfieren todos los datos en los volúmenes protegidos, que se denominan como una imagen base.

Para forzar una instantánea:

1. En la Core Console, haga clic en la pestaña **Machines (Máquinas)** y, a continuación, en la lista de máquinas protegidas, seleccione la máquina o clúster con el punto de recuperación en el que desea forzar una instantánea.
2. En el menú desplegable **Actions (Acciones)** de esa máquina, haga clic en **Force Snapshot (Forzar instantánea)** y, a continuación, seleccione una de las opciones que se describen a continuación:
   - **Force Snapshot (Forzar instantánea)**: toma una instantánea incremental de los datos actualizados desde que se tomó la última instantánea.
   - **Force Base Image (Forzar imagen base)**: toma una instantánea completa de los datos de los volúmenes de la máquina.
3. Cuando aparezca una notificación en el cuadro de diálogo **Transfer Status (Estado de transferencia)** de que la instantánea se ha puesto en cola, haga clic en **OK (Aceptar)**.

Aparecerá una barra de progreso junto a la máquina en la pestaña **Machines (Máquinas)** que mostrará el progreso de la instantánea.

Cómo pausar y reanudar la protección

Cuando se hace una pausa en la protección, se detienen temporalmente todas las transferencias de datos desde la máquina actual.

Para hacer una pausa y reanudar la protección:

1. En la Core Console, haga clic en la pestaña **Machines (Máquinas)**.
2. Seleccione la máquina en la que desea pausar la protección.
   Se abrirá la pestaña **Summary (Resumen)** para esta máquina.
3. En el menú desplegable **Actions (Acciones)** de esa máquina, haga clic en **Pause (Pausar)**.
4. Para reanudar la protección, haga clic en **Resume (Reanudar)** en el menú **Actions (Acciones)**.

Restablecimiento de datos

Puede recuperar o restaurar al instante datos en sus máquinas físicas (para máquinas Windows o Linux) o en máquinas virtuales a partir de puntos de recuperación almacenados para máquinas Windows. Los temas de esta sección describen cómo puede exportar un punto de recuperación específico para máquinas Windows a una máquina virtual o revertir una máquina a un punto de recuperación anterior.

Si ha configurado la replicación entre dos Cores (origen y destino), solo podrá exportar datos del Core de destino después de que la replicación inicial se haya completado. Para obtener más detalles, consulte Replicación de datos de Agent en una máquina.

NOTA: Los sistema operativos Windows 8 y Windows Server 2012 que se inician desde particiones FAT32 EFI no están disponibles para la recuperación o protección, ni tampoco los volúmenes del Sistema de archivos resistente (ReFS).

Acerca de la exportación de datos protegidos de máquinas de Windows a máquinas virtuales

AppAssure es compatible con la exportación puntual o continua (para admitir máquinas en espera virtuales) de información de copias de seguridad de Windows a una máquina virtual. La exportación de los datos a una máquina en espera virtual proporciona una copia de alta disponibilidad de los datos. Si una máquina protegida deja de funcionar, puede iniciar la máquina virtual para realizar la recuperación.

El siguiente diagrama muestra una implementación típica para la exportación de datos a una máquina virtual.

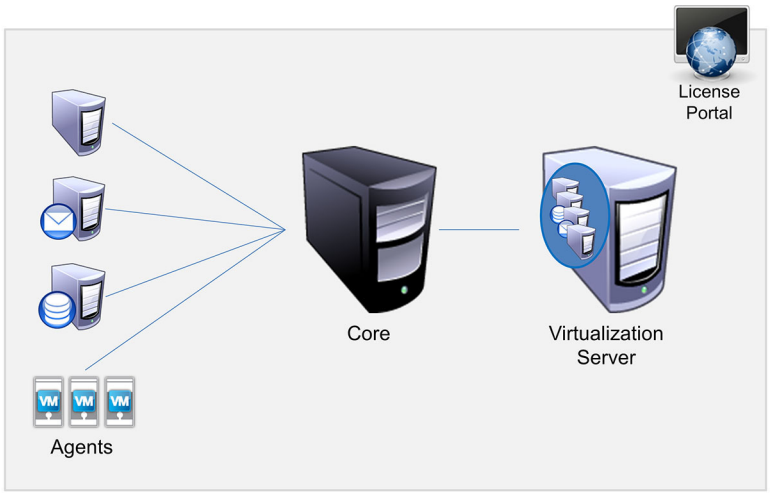

Ilustración 9. Exportación de datos a una máquina virtual

Para crear una máquina en espera virtual, se exportan datos protegidos de manera continua desde la máquina de Windows a una máquina virtual (VMware, ESXi o Hyper-V). Cuando se exporta a una máquina virtual, se exportan los datos de copia de seguridad de un punto de recuperación, así como los parámetros definidos en el programa de protección de la máquina.

NOTA: La máquina virtual a la que exporte deberá tener una versión con licencia de ESXi, estación de trabajo de VMWare o Hyper-V, en lugar de las versiones gratuitas o de prueba.

Limitaciones de compatibilidad de volúmenes básicos y dinámicos

AppAssure admite la toma de instantáneas de todos los volúmenes básicos y dinámicos. AppAssure también admite la exportación de los volúmenes dinámicos simples que están en un único disco físico. Como su nombre indica, los volúmenes dinámicos simples no son volúmenes seccionados, duplicados ni distribuidos. Los volúmenes que no son simples disponen de una geometría de disco arbitraria que no se puede interpretar por completo y, por lo tanto, no se pueden exportar. AppAssure posee la capacidad de exportar volúmenes dinámicos complejos o que no son simples.

En la interfaz de usuario de la versión 5.3.1.60393 de AppAssure se ha agregado una casilla de verificación que permite informar de que las exportaciones están limitadas a los volúmenes dinámicos simples. Antes de que la interfaz de usuario cambiara con esta versión, la opción de exportar discos dinámicos complejos o que no son simples podría haber sido una posibilidad. No obstante, si intentara exportar estos discos, la tarea de exportación hubiera generado un error.

Exportación de información de copia de seguridad de una máquina Windows a una máquina virtual

En AppAssure puede exportar datos desde sus máquinas Windows a una máquina virtual (VMWare, ESXi e Hyper-V) mediante la exportación de toda la información de copia de seguridad desde un punto de recuperación, así como de los parámetros definidos para el programa de protección de la máquina.

Para exportar la información de copia de seguridad de Windows a una máquina virtual:

1. En la Core Console, haga clic en la pestaña **Machines (Máquinas)**.
2. En la lista de máquinas protegidas, seleccione la máquina o clúster con el punto de recuperación para el que quiera exportar.

3. En el menú desplegable **Actions (Acciones)** para la máquina, haga clic en **Export (Exportar)** y, a continuación, seleccione el tipo de exportación que desee realizar. Puede elegir entre las siguientes opciones:
   - Exportación ESXi
   - Exportación VMware Workstation
   - Exportación Hyper-V

   Aparecerá el cuadro de diálogo **Select Export Type (Seleccionar tipo de exportación)**.

Exportación de datos de Windows mediante exportación ESXi

En AppAssure, puede elegir exportar datos mediante la exportación ESXi realizando una exportación única o continua.

Cómo realizar una exportación ESXi única

Para realizar una exportación ESXi única:

1. En el cuadro de diálogo **Select Export Type (Seleccionar tipo de exportación)**, haga clic en **One-time export (Exportación única)**.
2. Haga clic en **Siguiente**.
   Aparecerá el cuadro de diálogo **ESXi Export - Select Recovery Point (Exportación de ESXi: Seleccionar punto de recuperación)**.
3. Seleccione un punto de recuperación para exportar y, a continuación, haga clic en **Next (Siguiente)**.
   Aparecerá el cuadro de diálogo **Virtual Standby Recovery Point to VMware vCenter Server/ESXi (Punto de recuperación en espera virtual al VMware vCenter Server/ESXi)**.

Definición de la información de máquina virtual para realizar una exportación ESXi

Para definir la información de máquina virtual para realizar una exportación ESXi:

1. En el cuadro de diálogo **Virtual Standby Recovery Point to VMware vCenter Server/ESXi (Punto de recuperación en espera virtual al VMware vCenter Server/ESXi)**, introduzca los parámetros para acceder a la máquina virtual, tal como se describe a continuación:

Cuadro de texto	Descripción
Host Name (Nombre del host)	Introduzca un nombre para la máquina host.
Port	Introduzca el puerto para la máquina host. El puerto predeterminado es 443.
Nombre de usuario	Introduzca las credenciales de inicio de sesión para la máquina host.
Contraseña	Introduzca las credenciales de inicio de sesión para la máquina host.

2. Haga clic en **Connect (Conectar)**.

Cómo realizar una exportación ESXi continua (en espera virtual)

Para realizar una exportación ESXi continua (en espera virtual):

1. En el cuadro de diálogo **Select Export Type (Seleccionar tipo de exportación)**, haga clic en **Continuous (Virtual Standby) (Continua [en espera virtual])**.
2. Haga clic en **Next (Siguiente)**.

Se muestra el cuadro de diálogo **Virtual Standby Recovery Point to VMware vCenter Server/ESXi (Punto de recuperación en espera virtual para VMware vCenter Server/ESXi)**.

3. Introduzca los parámetros para acceder a la máquina virtual, tal como se describe a continuación.

Cuadro de texto	Descripción
Host Name (Nombre del host)	Introduzca un nombre para la máquina host.
Port	Introduzca el puerto para la máquina host. El puerto predeterminado es 443.
Nombre de usuario	Introduzca las credenciales de inicio de sesión para la máquina host.
Contraseña	Introduzca las credenciales de inicio de sesión para la máquina host.

4. Haga clic en Conectar.
5. En la pestaña **Options (Opciones)**, introduzca la información para la máquina virtual según lo descrito.

Cuadro de texto	Descripción
Virtual Machine Name (Nombre de máquina virtual)	Introduzca un nombre para la máquina virtual.
Memoria	Especifique el uso de la memoria. Puede elegir entre las siguientes opciones: • Use the same amount of RAM as source machine (Utilizar la misma cantidad de RAM que la máquina de origen) • Use a specific amount of RAM, and then specify the amount in MB (Utilizar una cantidad de RAM específica y, a continuación, especificar la cantidad en MB)
ESXi Datacenter (Centro de datos ESXi)	Introduzca el nombre para el centro de datos ESXi.
ESXi Host (Host ESXi)	Introduzca las credenciales para el host ESXi.
Data Store (Almacén de datos)	Introduzca los detalles para el almacén de datos.
Resource Pool (Grupo de recursos)	Introduzca un nombre para el grupo de recursos.

6. Haga clic en **Start Export (Iniciar exportación)**.

Exportación de datos de Windows mediante una exportación VMware Workstation

En AppAssure, puede seleccionar exportar datos mediante una exportación VMware Workstation al realizar una exportación única o continua. Complete los pasos que se indican en los siguientes procedimientos para exportar mediante una exportación VMware Workstation para el tipo de exportación adecuado.

Cómo realizar una exportación VMWare Workstation única

Para realizar una exportación VMWare Workstation única:

1. En el cuadro de diálogo **Select Export Type (Seleccionar tipo de exportación)**, haga clic en **One-time export (Exportación única)**.
2. Haga clic en **Next (Siguiente)**.
   Aparecerá el cuadro de diálogo **VM Export - Select Recovery Point (Exportación de VM: Seleccionar punto de recuperación)**.
3. Seleccione un punto de recuperación para exportar y, a continuación, haga clic en **Next (Siguiente)**.
   Aparecerá el cuadro de diálogo **Virtual Standby Recovery Point to VMware Workstation/Server (Punto de recuperación en espera virtual a estación de trabajo/servidor de VMware)**.

Definición de configuración única para realizar una exportación VMware Workstation

Para definir la configuración única para realizar una exportación VMware Workstation:

1. En el cuadro de diálogo **Virtual Standby Recovery Point to VMware Workstation/Server (Punto de recuperación en espera virtual a estación de trabajo/servidor de VMware)**, introduzca los parámetros para acceder a la máquina virtual, según se describe a continuación:

Cuadro de texto	Descripción
Target Path (Ruta de acceso de destino)	Especifique la ruta de acceso de la carpeta local o recurso compartido de red en el que crear la máquina virtual. NOTA: Si especificó una ruta de acceso de recurso compartido de red, introduzca credenciales de inicio de sesión válidas para una cuenta que esté registrada en la máquina de destino. La cuenta debe tener permisos de lectura y escritura para el recurso compartido de red.
User Name (Nombre de usuario)	Introduzca las credenciales de inicio de sesión para la máquina virtual. • Si ha especificado una ruta de acceso de recurso compartido de red, debe introducir un nombre de usuario válido para una cuenta registrada en la máquina de destino. • Si ha especificado una ruta de acceso local, no hace falta nombre de usuario.
Contraseña	Introduzca las credenciales de inicio de sesión para la máquina virtual. • Si ha especificado una ruta de acceso de recurso compartido de red, debe introducir una contraseña válida para una cuenta registrada en la máquina de destino. • Si ha especificado una ruta de acceso local, no hace falta contraseña.

2. En el panel **Export Volumes (Exportar volúmenes)**, seleccione los volúmenes a exportar; por ejemplo, C:\ y D:\.
3. En el panel Options (Opciones), introduzca la información para la máquina virtual y el uso de la memoria, tal y como se describe a continuación:

Cuadro de texto	Descripción
Virtual Machine (Máquina virtual)	Introduzca un nombre para la máquina virtual que se está creando. Por ejemplo, VM-0A1B2C3D4. NOTA: El nombre predeterminado es el nombre de la máquina origen.
Memoria	Especifique la memoria para la máquina virtual. • Haga clic en **Use the same amount of RAM as the source machine (Utilizar la misma cantidad de RAM que la máquina de origen)** para especificar que la configuración de RAM es la misma que en la máquina de origen. • Haga clic en **Use a specific amount of RAM (Utilizar una cantidad de RAM específica)** para especificar la cantidad de RAMque utilizar. Por ejemplo, 4096 MB. La cantidad mínima permitida es 512 MB y la máxima viene determinada por la capacidad y las limitaciones de la máquina host.

4. Haga clic en **Export (Exportar)**.

Cómo realizar una exportación VMware Workstation continua (en espera virtual)

Para realizar una exportación VMware Workstation continua (en espera virtual):

1. En el cuadro de diálogo **Select Export Type (Seleccionar tipo de exportación)**, haga clic en **Continuous (Virtual Standby) (Continua [en espera virtual])** y, a continuación, haga clic en **Next (Siguiente)**.

   Aparecerá el cuadro de diálogo **VM Export - Select Recovery Point (Exportación de VM: Seleccionar punto de recuperación)**.
2. Seleccione un punto de recuperación para exportar y, a continuación, haga clic en **Next (Siguiente)**.

   Aparecerá el cuadro de diálogo **Virtual Standby Recovery Point to VMware Workstation/Server (Punto de recuperación en espera virtual a estación de trabajo/servidor de VMware)**.
3. Introduzca los parámetros para acceder a la máquina virtual, tal como se describe a continuación:

Cuadro de texto	Descripción
Target Path (Ruta de acceso de destino)	Especifique la ruta de acceso de la carpeta local o recurso compartido de red en el que crear la máquina virtual. NOTA: Si especificó una ruta de acceso de recurso compartido de red, introduzca credenciales de inicio de sesión válidas para una cuenta que esté registrada en la máquina de destino. La cuenta debe tener permisos de lectura y escritura para el recurso compartido de red.
User Name (Nombre de usuario)	Introduzca las credenciales de inicio de sesión para la máquina virtual. • Si ha especificado una ruta de acceso de recurso compartido de red, debe introducir un nombre de usuario válido para una cuenta registrada en la máquina de destino. • Si ha especificado una ruta de acceso local, no hace falta nombre de usuario.
Contraseña	Introduzca las credenciales de inicio de sesión para la máquina virtual.

Cuadro de texto	Descripción
	• Si ha especificado una ruta de acceso de recurso compartido de red, debe introducir una contraseña válida para una cuenta registrada en la máquina de destino. • Si ha especificado una ruta de acceso local, no hace falta contraseña.

4. En el panel **Export Volumes (Exportar volúmenes)**, seleccione los volúmenes a exportar; por ejemplo, **C:** y **D:**.
5. En el panel **Options (Opciones)**, introduzca la información para la máquina virtual y el uso de la memoria, tal y como se describe en la siguiente tabla.

Cuadro de texto	Descripción
Virtual Machine (Máquina virtual)	Introduzca un nombre para la máquina virtual que se está creando. Por ejemplo, `VM-0A1B2C3D4`. **NOTA:** El nombre predeterminado es el nombre de la máquina origen.
Memoria	Especifique la memoria para la máquina virtual. • Haga clic en **Use the same amount of RAM as the source machine (Utilizar la misma cantidad de RAM que la máquina de origen)** para especificar que la configuración de RAM es la misma que en la máquina de origen. • Haga clic en **Use a specific amount of RAM (Utilizar una cantidad de RAM específica)** para especificar la cantidad de RAMque desea utilizar; por ejemplo, 4096 MB. La cantidad mínima permitida es 512 MB y la máxima viene determinada por la capacidad y las limitaciones de la máquina host.

6. Haga clic en **Perform initial ad-hoc export (Realizar exportación ad hoc-inicial)** para probar la exportación de los datos.
7. Haga clic en **Save (Guardar)**.

Exportación de datos de Windows mediante exportación Hyper-V

Puede exportar datos mediante exportación de Hyper-V realizando una exportación única o continua. Lleve a cabo los pasos de los procedimientos siguientes para exportar mediante exportación de Hyper-V con el tipo adecuado de exportación.
El appliance DL es compatible con la primera generación de exportación de Hyper-V a los siguientes hosts:

- Windows 8
- Windows 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

El appliance DL es compatible con la segunda generación de exportación de Hyper-V a los siguientes hosts:

- Windows 8.1
- Windows Server 2012 R2

NOTA: No todas las máquinas protegidas pueden ser exportadas a hosts Hyper-V de segunda generación.

Solo las máquinas protegidas con los siguientes sistemas operativos Unified Extensible Firmware Interface (UEFI) admiten la exportación virtual a hosts Hyper-V de segunda generación:

- Windows 8 (UEFI)
- Windows 8.1 (UEFI)
- Windows Server 2012 UEFI
- Windows Server 2012R2 (UEFI)

NOTA: La exportación Hyper-V a VM de segunda generación puede fallar si el host Hyper-V no tiene suficiente RAM asignada al realizar la exportación.

Realice los pasos de los procedimientos siguientes para el tipo de exportación adecuado.

Cómo realizar una exportación Hyper-V única

Para realizar una exportación Hyper-V única:

1. En la Core Console, navegue a la máquina que desee exportar.
2. En la ficha Summary (Resumen), haga clic en **Actions** → **Export** → **One-time** (Acciones > Exportar > Una vez).

   El asistente **Export Wizard (Asistente de exportación)** se muestra en la página **Protected Machines (Máquinas protegidas)**.
3. Seleccione una máquina para exportarla y, a continuación, haga clic en **Next (Siguiente)**.
4. En la página **Recovery Points (Puntos de recuperación)**, seleccione el punto de recuperación que desea exportar y, a continuación, haga clic en **Next (Siguiente)**.

Definición de configuración única para realizar una exportación Hyper-V

Para definir la configuración única para realizar una exportación Hyper-V:

1. En el cuadro de diálogo Hyper-V, haga clic en **Use local machine (Utilizar máquina local)** para realizar la exportación Hyper-V a una máquina local con la función Hyper-V asignada.
2. Haga clic en la opción **Remote host (Host remoto)** para indicar que el servidor de Hyper-V se encuentra en una máquina remota. Si ha seleccionado la opción Remote host (Host remoto), introduzca los parámetros del host remoto, según se describe a continuación:

Cuadro de texto	Descripción
Host Name	Introduzca una dirección IP o un nombre de host para el servidor de Hyper-V. Representa la dirección IP o el nombre de host del servidor de Hyper-V remoto.
Port	Introduzca un número de puerto para la máquina. Representa el puerto a través del cuál el Core se comunica con esta máquina.
User Name	Introduzca el nombre de usuario para el usuario con privilegios administrativos para la estación de trabajo con el servidor de Hyper-V. Se utiliza para especificar las credenciales de inicio de sesión para la máquina virtual.

Cuadro de texto	Descripción
Password	Introduzca la contraseña de la cuenta de usuario con privilegios administrativos en la estación de trabajo con el servidor de Hyper-V. Se utiliza para especificar las credenciales de inicio de sesión para la máquina virtual.

3. Haga clic en **Next (Siguiente)**.
4. En la página **Virtual Machines Options (Opciones de máquinas virtuales)**, especifique la ruta de acceso a la máquina virtual en el cuadro de texto VM Machine Location (Ubicación de la máquina virtual); por ejemplo, **D:\export** (D:\exportación). Se utiliza para identificar la ubicación de la máquina virtual.
5. Escriba el nombre de la máquina virtual en el campo **Virtual Machine Name (Nombre de la máquina virtual)**.

   El nombre que especifique aparece en la lista de máquinas virtuales en la consola Hyper-V Manager (Administrador de Hyper-V).
6. Haga clic en una de las opciones siguientes:
   - **Use the same amount of RAM as the source machine (Utilizar la misma cantidad de RAM que la máquina de origen)**, para identificar que el uso de RAM es idéntico entre la máquina virtual y la máquina de origen.
   - **Use a specific amount of RAM (Utilizar una cantidad específica de RAM)**, para especificar la cantidad de memoria que la máquina virtual debería tener tras la exportación; por ejemplo, 4096 MB.
7. Para especificar el formato del disco, junto a **Disk Format (Formato de disco)**, haga clic en una de las opciones siguientes:
   - **VHDX**
   - **VHD**

   NOTA: La exportación Hyper-V admite formatos de disco VHDX si la máquina de destino ejecuta Windows 8 (Windows Server 2012) o superior. Si el formato VHDX no es compatible para su entorno, la opción estará desactivada.
8. En la página **Volumes (Volúmenes)**, seleccione los volúmenes que se van a exportar, por ejemplo, C:\.

   Para VHD, los volúmenes seleccionados no deberían tener un tamaño superior a 2040 GB. Si los volúmenes seleccionados tienen un tamaño de más de 2040 GB y se selecciona el formato VHD, recibirá un mensaje de error.
9. En la página **Summary (Resumen)**, haga clic en **Finish (Finalizar)** para completar el asistente y para iniciar la exportación.

Cómo realizar una exportación Hyper-V continua (en espera virtual)

Para realizar una exportación Hyper-V continua (en espera virtual):

1. En la Core Console, en la ficha **Virtual Standby (En espera virtual)**, haga clic en **Add (Agregar)** para iniciar el asistente **Export Wizard (Asistente de exportación)**. En la página **Protected Machines (Máquinas protegidas)** del **Export Wizard (Asistente de exportación)**.
2. Seleccione la máquina que desea exportar y, a continuación, haga clic en **Next (Siguiente)**.
3. En la ficha **Summary (Resumen)**, haga clic en **Export → Virtual Standby (Exportar > En espera virtual)**.
4. En el cuadro de diálogo Hyper-V, haga clic en **Use local machine (Utilizar máquina local)** para realizar la exportación Hyper-V a una máquina local con la función Hyper-V asignada.
5. Haga clic en la opción **Remote host (Host remoto)** para indicar que el servidor de Hyper-V se encuentra en una máquina remota. Si ha seleccionado la opción Remote host (Host remoto), introduzca los parámetros del host remoto, según se describe a continuación:

Cuadro de texto	Descripción
Host Name	Introduzca una dirección IP o un nombre de host para el servidor de Hyper-V. Representa la dirección IP o el nombre de host del servidor de Hyper-V remoto.
Port	Introduzca un número de puerto para la máquina. Representa el puerto a través del cuál el Core se comunica con esta máquina.
User Name	Introduzca el nombre de usuario para el usuario con privilegios administrativos para la estación de trabajo con el servidor de Hyper-V. Se utiliza para especificar las credenciales de inicio de sesión para la máquina virtual.
Password	Introduzca la contraseña de la cuenta de usuario con privilegios administrativos en la estación de trabajo con el servidor de Hyper-V. Se utiliza para especificar las credenciales de inicio de sesión para la máquina virtual.

6. En la página **Virtual Machines Options (Opciones de máquinas virtuales)**, especifique la ruta de acceso a la máquina virtual en el cuadro de texto VM Machine Location (Ubicación de la máquina virtual); por ejemplo, **D:\export** (D:\exportación). Se utiliza para identificar la ubicación de la máquina virtual.
7. Escriba el nombre de la máquina virtual en el campo **Virtual Machine Name (Nombre de la máquina virtual)**.

   El nombre que especifique aparece en la lista de máquinas virtuales en la consola Hyper-V Manager (Administrador de Hyper-V).
8. Haga clic en una de las opciones siguientes:
   - **Use the same amount of RAM as the source machine (Utilizar la misma cantidad de RAM que la máquina de origen)**, para identificar que el uso de RAM es idéntico entre la máquina virtual y la máquina de origen.
   - **Use a specific amount of RAM (Utilizar una cantidad específica de RAM)**, para especificar la cantidad de memoria que la máquina virtual debería tener tras la exportación; por ejemplo, 4096 MB.
9. Para especificar el formato del disco, junto a **Disk Format (Formato de disco)**, haga clic en una de las opciones siguientes:
   - **VHDX**
   - **VHD**

   NOTA: La exportación Hyper-V admite formatos de disco VHDX si la máquina de destino ejecuta Windows 8 (Windows Server 2012) o superior. Si el formato VHDX no es compatible para su entorno, la opción estará desactivada.
10. En la página **Volumes (Volúmenes)**, seleccione los volúmenes que se van a exportar, por ejemplo, C:\.

    Para VHD, los volúmenes seleccionados no deberían tener un tamaño superior a 2040 GB. Si los volúmenes seleccionados tienen un tamaño de más de 2040 GB y se selecciona el formato VHD, recibirá un mensaje de error.
11. Seleccione **Perform initial ad-hoc export (Realizar exportación ad hoc inicial)**, para realizar la exportación virtual inmediatamente en lugar de después de la siguiente instantánea programada.
12. En la página **Summary (Resumen)**, haga clic en **Finish (Finalizar)** para completar el asistente y para iniciar la exportación.

    NOTA: Para supervisar el estado y el progreso de la exportación, visualice **Virtual Standby (En espera virtual)** o la ficha **Events (Eventos)**.

Cómo realizar una reversión

En AppAssure, una reversión es el proceso de restauración de los volúmenes en una máquina desde puntos de recuperación.

NOTA: La funcionalidad de reversión también se admite para máquinas Linux mediante el uso de la utilidad de línea de comandos `aamount`. Para obtener más información, consulte Cómo realizar una reversión para una máquina Linux mediante la línea de comandos.

Para realizar una reversión:

1. En la Core Console, realice una de las acciones siguientes:
   - Haga clic en la pestaña **Machines (Máquinas)**, y siga estos pasos:

   a. En la lista de máquinas protegidas, seleccione la casilla de verificación junto a la máquina que desee exportar.
   b. En el menú desplegable **Actions (Acciones)** de esa máquina, haga clic en **Rollback (Revertir)**.
   c. En el cuadro de diálogo **Rollback — Select Recovery Point (Reversión: seleccionar punto de recuperación)**, seleccione el punto de recuperación que desea exportar y haga clic en **Next (Siguiente)**.
      - En el área de navegación izquierda de la AppAssure 5 Core Console, seleccione la máquina que desea revertir. Se abrirá la pestaña **Summary (Resumen)** de la máquina.
   d. Haga clic en la pestaña **Recovery Points (Puntos de recuperación)** y, a continuación, seleccione un punto de recuperación de la lista.
   e. Expanda los detalles de ese punto de recuperación y haga clic en **Rollback (Revertir)**.
2. Edite las opciones de reversión como se describe en la tabla siguiente.

Cuadro de texto	Descripción
Protected Machine (Máquina protegida)	Especifica la máquina del Agent original como el destino de la reversión. El origen se refiere al Agent en el que se creó el punto de recuperación que se va a usar para la reversión.
Recovery Console Instance (Instancia de consola de recuperación)	Para restaurar el punto de recuperación en cualquier máquina que se haya iniciado en modo URC, introduzca el nombre de usuario y la contraseña.

3. Haga clic en **Load Volumes (Cargar volúmenes)**.
   Aparecerá el cuadro de diálogo **Volume Mapping (Asignación de volúmenes)**.

   NOTA: La Core Console no asigna volúmenes de Linux automáticamente. Para buscar un volumen de Linux, vaya al volumen que desea revertir.
4. Seleccione los volúmenes que desea revertir.
5. Use la opción **Destination (Destino)** para seleccionar el volumen de destino en el que desea revertir el volumen seleccionado.
6. Seleccione una de las opciones siguientes:
   - **Live Recovery (Recuperación directa)**. Al seleccionar esta opción, la reversión de los volúmenes de Windows se produce de manera inmediata. Esta es la configuración predeterminada.

     NOTA: La opción **Live Recovery (Recuperación directa)** no está disponible para los volúmenes de Linux.
   - **Force Dismount (Forzar desmontaje)**. Esta opción fuerza el desmontaje de los puntos de recuperación montados antes de realizar la reversión. Esta es la configuración predeterminada.

7. Haga clic en **Rollback (Revertir)**.

   El sistema comienza a procesar la reversión al punto de recuperación seleccionado.

Cómo realizar una reversión para una máquina Linux mediante la línea de comandos

Una reversión es el proceso de restaurar los volúmenes de una máquina a partir de puntos de recuperación. En AppAssure, puede realizar una reversión para los volúmenes de sus máquinas Linux protegidas mediante la utilidad de línea de comandos `aamount`.

PRECAUCIÓN: No intente realizar una reversión en el volumen raíz (/) o en el sistema.

NOTA: La función de reversión es compatible con máquinas Windows protegidas de la Core Console. Para obtener más información, consulte Cómo realizar una reversión.

Para realizar una reversión de un volumen en una máquina Linux:

1. Ejecute la utilidad `aamount` de AppAssure como raíz, por ejemplo:

   ```
   sudo aamount
   ```

2. En la solicitud de montaje de AppAssure, introduzca el siguiente comando para enumerar las máquinas protegidas:

   ```
   lm
   ```

3. Cuando se le solicite, introduzca la dirección IP o nombre del host del servidor AppAssure Core.
4. Introduzca las credenciales de inicio de sesión, es decir, el nombre de usuario y la contraseña, para este servidor.

   Se muestra una lista con las máquinas que el servidor de AppAssure protege. En la lista, aparecerán las máquinas de Agent encontradas por número de elemento de línea, host/dirección IP y el número de Id. de la máquina (por ejemplo: `293cc667-44b4-48ab-91d8-44bc74252a4f`).

5. Para ver los puntos de recuperación montados actualmente de la máquina especificada, introduzca el siguiente comando:

   ```
   lr <machine_line_item_number>
   ```

   NOTA: También puede introducir el número de Id. de la máquina en lugar del número de elemento de línea.

   Aparece una lista que muestra los puntos de recuperación básicos e incrementales de dicha máquina. Esta lista incluye un número de elemento de línea, fecha/fecha y hora, ubicación de volumen, tamaño de punto de recuperación y un número de Id. para el volumen que incluye un número de secuencia al final (por ejemplo, ”`293cc667-44b4-48ab-91d8-44bc74252a4f:2`”), que identifica el punto de recuperación.

6. Para seleccionar el punto de recuperación que se va a revertir, introduzca el siguiente comando:

   ```
   r [volume_recovery_point_ID_number] [path]
   ```

   Este comando revierte la imagen de volumen especificada por el Id. del Core en la ruta de acceso especificada. La ruta de acceso para la reversión es la ruta de acceso para el descriptor de archivo de dispositivo y no el directorio en el que está montado.

NOTA: Para identificar el punto de recuperación, también puede especificar un número de línea en el comando en lugar del número de Id. de punto de recuperación. En dicho caso, utilice el número de línea de máquina/Agent (en la salida de `lm`), seguido del número de línea de punto de recuperación y de la letra del volumen, seguido de la ruta de acceso, por ejemplo, `r [machine_line_item_number] [recovery_point_line_number] [volume_letter] [path]`. En este comando, [ruta] es el descriptor de archivo del volumen real.

Por ejemplo, si la salida de `lm` muestra tres máquinas de Agent, ha introducido el comando `lr` para el número 2 y desea revertir el volumen b del punto de recuperación 23 al volumen que se montó en el directorio `/mnt/data`, el comando será: `r2 23 b /mnt/data`.

NOTA: Es posible revertir a /, pero solo cuando se realiza una restauración desde cero mientras se inicia con un Live CD. Para obtener más información, consulte Cómo realizar una restauración desde cero para una máquina Linux.

7. Si se le solicita que continúe, escriba `y` para Sí.

   Mientras continúe la reversión, aparecerán una serie de mensajes para notificarle el estado.

8. Tras una reversión satisfactoria, la utilidad `aamount` monta automáticamente el módulo de núcleo y vuelve a conectarlo al volumen revertido si el destino estaba previamente protegido y montado. Si no, monte el volumen de reversión en el disco local y, a continuación, verifique que los archivos estén restaurados.

   Por ejemplo, puede usar el comando `sudo mount` y, a continuación, el comando `ls`.

   PRECAUCIÓN: No desmonte un volumen Linux protegido manualmente. En caso de que necesite hacerlo, debe ejecutar el siguiente comando antes de desmontar el volumen: `bsctl -d [path to volume]`.

   En este comando, [path to volume] no se hace referencia al punto de montaje del volumen sino al descriptor de archivo del volumen;debe tener un formato similar a: `/dev/sda1`.

Acerca de la restauración desde cero para máquinas Windows

Los servidores, cuando funcionan según lo esperado, ejecutan y realizan tareas para las que están configurados. Solo cuando fallan, la cosa cambia. Cuando se produce un evento catastrófico que vuelve el servidor inoperable, es necesario llevar a cabo pasos inmediatos para restaurar el servidor a su condición operativa anterior. El proceso normalmente entraña reformatear la máquina, reinstalar el sistema operativo, recuperar los datos a través de copias de seguridad y reinstalar las aplicaciones de software.

AppAssure ofrece la posibilidad de realizar una restauración desde cero (BMR) de las máquinas Windows, independientemente de que el hardware sea similar o distinto. Este proceso conlleva la creación de una imagen de CDde inicio, grabar la imagen en disco, iniciar el servidor de destino desde el disco, conectarse a la instancia de la consola de recuperación, asignar volúmenes, inicializar la recuperación y, a continuación, supervisar el proceso. Una vez terminada la restauración desde cero, podrá continuar con la tarea de cargar el sistema operativo y las aplicaciones de software en el servidor restaurado, seguida de sus valores y configuración únicos.

Otras circunstancias en las que puede decidir realizar una restauración desde cero incluyen una actualización de hardware o la sustitución del servidor.

La funcionalidad BMR también es compatible con las máquinas protegidas Linux gracias a la utilidad de línea de comandos `aamount`. Para obtener más información, consulte Cómo realizar una restauración desde cero para una máquina Linux.

Requisitos previos para realizar una restauración completa para una máquina Windows

Antes de empezar el proceso de la restauración desde cero para una máquina Windows, deberá asegurarse de que se cumplen las condiciones y criterios siguientes:

- Copias de seguridad del servidor y el Core en funcionamiento
- Hardware que se va a restaurar (nuevo o antiguo, similar o diferente)
- Software de grabación de CD y CD en blanco
- Visor VNC (opcional)
- Controladores de almacenamiento compatibles con Windows 7 PE (32 bit) y controladores de red para la máquina de destino.
- Controladora de almacenamiento, RAID, AHCI y controladores de chipset para el sistema operativo de destino

NOTA: Los controladores de la controladora de almacenamiento solo se necesitan si la restauración que se lleva a cabo es de hardware diferente.

Plan para realizar una restauración desde cero para una máquina Windows

Para realizar una restauración desde cero -BMR para una máquina Windows:

1. Cree un CD de inicio. Consulte Creación de una imagen ISO de un CD de inicio.
2. Grabe la imagen en el disco.
3. Inicie el servidor de destino desde el CD de inicio. Consulte Cómo cargar un CD de inicio.
4. Conéctese al disco de recuperación.
5. Asigne los volúmenes. Consulte Asignación de volúmenes.
6. Inicie la recuperación. Consulte Cómo iniciar una restauración desde el AppAssure Core.
7. Supervise el progreso. Consulte Visualización del progreso de la recuperación.

Creación de la imagen ISO de un CD de inicio

Para realizar una restauración completa (BMR) en una máquina de Windows, cree primero una imagen de CD/ISO de inicio en la Core Console, que contenga la interfaz de la AppAssure Universal Recovery Console (Consola de recuperación universal de AppAssure). Esta Consola es un entorno que permite restaurar una unidad del sistema o todo el servidor directamente desde el AppAssure Core.

La imagen ISO que cree se adapta a la máquina que se va a restaurar; por lo tanto, debe incluir los controladores de almacenamiento masivo y red correctos. Si piensa que va a restaurar en un hardware diferente al de la máquina en la que creará el CD de inicio, deberá incluir una controladora de almacenamiento y otros controladores en el CD de inicio. Consulte Inserción de controladores en un CD de inicio

NOTA: La Organización Internacional de Normalización (ISO) es un organismo internacional de representantes de diversas organizaciones nacionales que determinan y establecen los estándares de sistema de archivos. La ISO 9660 es un estándar de sistema de archivos que se utiliza con medios de disco óptico para el intercambio de datos y que admite diversos sistemas operativos, como por ejemplo, Windows. Una imagen ISO es el archivo de archivado o imagen de disco, que contiene datos de cada sector del disco, así como el sistema de archivos de disco.

Para crear una imagen ISO de un CD de inicio:

1. En la Core Console en la que se ubica el servidor que desea restaurar, seleccione el **Core** y, a continuación, haga clic en la ficha **Tools (Herramientas)**.
2. Haga clic en **Boot CDs (CD de inicio)**.
3. Seleccione **Actions (Acciones)** y, a continuación, haga clic en **Create Boot ISO (Crear ISO de inicio)**.

   Aparecerá el cuadro de diálogo **Create Boot CD (Crear CD de inicio)**. Para completar el cuadro de diálogo, realice los siguientes procedimientos.

Asignación de nombre del archivo del CD de inicio y configuración de la ruta de acceso

Para asignar un nombre al archivo del CD de inicio y configurar la ruta de acceso:

En el cuadro de diálogo **Create Boot CD (Crear CD de inicio)**, especifique la ruta ISO donde se almacenará la imagen de inicio en el servidor del Core.

Si al recurso compartido en el que desea almacenar la imagen le queda poco espacio, puede establecer la ruta de acceso según sea necesario; por ejemplo, D:\filename.iso.

NOTA: La extensión del archivo debe ser .iso. Al especificar la ruta, escriba solo caracteres alfanuméricos, un guión o un punto (para separar los nombres de host de los dominios). Las letras de la "a" a la "z" no distinguen mayúsculas de minúsculas. No utilice espacios. No se admite ningún otro símbolo o caracteres de puntuación.

Creación de conexiones

Para crear conexiones:

1. En **Connection Options (Opciones de conexión)**, haga lo siguiente:
   - Para obtener la dirección IP de manera dinámica mediante el Protocolo de configuración dinámica de host (DHCP), seleccione **Obtain IP address automatically (Obtener dirección IP automáticamente)**.
   - De manera opcional, para especificar una dirección IP estática para la consola de recuperación, seleccione **Use the following IP address (Usar la siguiente dirección IP)** y escriba la dirección IP, la máscara de subred, la puerta de enlace predeterminada y el servidor DNS en los campos correspondientes. Deberá introducir todos los campos.
2. Si se le solicita, en **UltraVNC Options (Opciones de UltraVNC)**, seleccione **Add UltraVNC (Agregar UltraVNC)** y, a continuación, escriba las opciones UltraVNC. La configuración de UltraVNC permite administrar la consola de recuperación de manera remota mientras se usa.

   NOTA: Este paso es opcional. Si necesita acceso remoto a la consola de recuperación, deberá configurar y usar UltraVNC. No podrá iniciar sesión con Microsoft Terminal Services mientras utiliza el CDde inicio.

Inserción de controladores en un CD de inicio

La inserción del controlador se utiliza para facilitar la operabilidad entre la consola de recuperación, el adaptador de red y el almacenamiento en el servidor de destino.

Si piensa que va a restaurar en hardware diferente, deberá incluir una controladora de almacenamiento, un disco RAID, una interfaz AHCI, un conjunto de chips u otros controladores en el CD de inicio. Estos controladores permiten que el sistema operativo detecte todos los dispositivos y funcione correctamente en ellos.

NOTA: Tenga en cuenta que el CD de inicio incluye controladores de Windows 7 PE de 32 bits de manera automática.

Para insertar controladores en un CD de inicio:

1. Descargue los controladores del sitio web del fabricante para el servidor y descomprímalos.
2. Comprima la carpeta que contiene los controladores mediante una utilidad de compresión de archivos, por ejemplo, WinZip.
3. En el cuadro de diálogo **Create Boot CD (Crear CD de inicio)**, en el panel **Drivers (Controladores)**, haga clic en **Add a Driver (Agregar un controlador)**.
4. Para buscar el archivo de controladores comprimido, vaya al sistema de archivos. Seleccione el archivo y haga clic en **Open (Abrir)**.

   Los controladores insertados se resaltan en el panel **Drivers (Controladores)**.

Creación del CD de inicio

Para crear un CD de inicio, asígnele un nombre y especifique una ruta y, después, cree una conexión e inserte los controladores de manera opcional. En la pantalla **Create Boot CD (Crear CD de inicio)**, haga clic en **Create Boot CD (Crear CD de inicio)**. A continuación, se creará la imagen ISO.

Visualización del progreso de creación de la imagen ISO

Para ver el progreso de la creación de la imagen ISO, seleccione la pestaña **Events (Eventos)** y, a continuación en **Tasks (Tareas)**, puede supervisar el progreso para crear una imagen ISO.

NOTA: También puede ver el progreso de la creación de la imagen ISO en el cuadro de texto **Monitor Active Task (Supervisar tarea activa)**.

Cuando la creación de la imagen ISO esté completada, estará disponible en la página **Boot CDs (CD de inicio)**, a la que se puede acceder desde el menú **Tools (Herramientas)**.

Acceso a la imagen ISO

Para acceder a la imagen ISO, navegue a la rutade acceso de salida que ha especificado, o bien haga clic en el enlace para descargar la imagen en una ubicación desde la que podrá cargarla al nuevo sistema. Por ejemplo, una unidad de red.

Cómo cargar un CD de inicio

Cuando haya creado la imagen del CD de inicio, inicie el servidor de destino con el CD de inicio que acaba de crear.

NOTA: Si ha creado el CD de inicio mediante DHCP, anote la dirección IP y la contraseña.

Para cargar un CD de inicio:

1. Vaya al nuevo servidor, cargue el CD de inicio e inicie la máquina.
2. Elija **Boot from CD-ROM (Iniciar desde el CD-ROM)**, que cargará lo siguiente:
   - Windows 7 PE
   - Software AppAssure 5 Agent

Se inicia la AppAssure Universal Recovery Console (Consola de recuperación universal) y muestra la dirección IP y la contraseña de autenticación de la máquina.

3. Anote la dirección IP que aparece en el panel Network Adapters Settings (Configuración de adaptadores de red) y la contraseña de autenticación que se muestra en el panel Authentication (Autenticación). Necesitará esta información más adelante, durante el proceso de recuperación de datos, para volver a iniciar sesión en la consola.
4. Si desea cambiar la dirección IP, selecciónela y haga clic en **Change (Cambiar)**.

   NOTA: Si especificó una dirección IP en el cuadro de diálgo Create Boot CD (Crear CD de inicio), la Universal Recovery Console la utiliza y la muestra en la pantalla **Network Adapters Settings (Configuración de adaptadores de red)**.

Inserción de controladores en el servidor de destino

Si va a restaurar en hardware diferente, debe insertar una controladora de almacenamiento, un disco RAID, una interfaz AHCI, un conjunto de chips u otros controladores, en caso de que aún no estén incluidos en el CD de inicio. Estos controladores permiten que el sistema operativo funcione en todos los dispositivos del servidor de destino correctamente.

Si desconoce los controladores que requiere su servidor de destino, haga clic en la pestaña System Info (Información del sistema) en la Consola de recuperación universal. En esta pestaña se muestran todos los tipos de dispositivo y de hardware de sistema del servidor de destino que desea restaurar.

NOTA: Tenga en cuenta que el servidor de destino incluye controladores de Windows 7 PE de 32 bits de manera automática.

Para insertar controladores en el servidor de destino:

1. Descargue los controladores del sitio web del fabricante para el servidor y descomprímalos.
2. Comprima la carpeta que contiene los controladores mediante una utilidad de compresión de archivos (por ejemplo, Win Zip) y cópiela en el servidor de destino.
3. En la Consola de recuperación universal, haga clic en **Driver Injection (Inserción de controlador)**.
4. Para buscar el archivo de controladores comprimido, vaya al sistema de archivos y selecciónelo.
5. Si hizo clic en **Driver Injection (Inserción de controlador)** en el paso 3, haga clic en **Add Driver (Agregar controlador)**. Si eligió **Load driver (Cargar controlador)** en el paso 3, haga clic en **Open (Abrir)**.

   Los controladores seleccionados se insertarán y se cargarán en el sistema operativo después de reiniciar el servidor de destino.

Cómo iniciar una restauración desde el Core

Para iniciar una restauración desde el Core:

1. Si las NIC de cualquier sistema que se estén restaurando están en equipo (asociadas), quite todas salvo una de los cables de red.

   NOTA: La restauración de AppAssure no reconoce NICen equipo. El proceso no puede resolver qué NIC usar si está presente con más de una conexión activa.
2. Vuelva al servidor del Core y abra la Core Console.
3. En la pestaña **Machines (Máquinas)**, seleccione la máquina desde la que desea restaurar datos.
4. Haga clic en el menú **Actions (Acciones)** de la máquina, haga clic en **Recovery Points (Puntos de recuperación)** para ver una lista de todos los puntos de recuperación de esa máquina.
5. Expanda el punto de recuperación desde el que desea restaurar y, a continuación, haga clic en **Rollback (Revertir)**.

6. En el cuadro de diálogo **Rollback (Revertir)**, en **Choose Destination (Elegir destino)**, seleccione **Recovery Console Instance (Instancia de la consola de recuperación)**.
7. En los cuadros de texto **Host** y **Password (Contraseña)**, introduzca la dirección IP y la contraseña de autentificación del nuevo servidor en el que desea restaurar datos.

   NOTA: Los valores de Host y Password (Contraseña) son las credenciales que ha grabado en la tarea anterior. Para obtener más información, ver Cómo cargar un CD de inicio.
8. Haga clic en **Load Volumes (Cargar volúmenes)** para cargar los volúmenes de destino en la nueva máquina.

Asignación de volúmenes

Puede asignar volúmenes a los discos del servidor de destino de forma automática o manual. Para alinear los discos automáticamente, el disco se debe limpiar y volver a particionar y todos los datos se eliminarán. La alineación se realiza en el orden en que aparecen los volúmenes, y éstos se asignan a los discos según convenga en función del tamaño, etc. Varios volúmenes pueden usar un disco. Si asigna unidades manualmente, no podrá usar el mismo disco dos veces.

Para la asignación manual, debe tener la máquina nueva con el formato correcto antes de restaurarla. Para obtener más información, consulte Cómo iniciar una restauración desde el AppAssure Core.

Para asignar volúmenes:

1. Para asignar volúmenes automáticamente, realice estos pasos:
   a. En el cuadro de diálogo **RollbackURC**, seleccione la pestaña **Automatically Map Volumes (Asignar volúmenes automáticamente)**.
   b. En el área **Disk Mapping (Asignación de discos)**, en **Source Volume (Volumen de origen)**, compruebe que el volumen de origen está seleccionado y que los volúmenes adecuados aparecen debajo y están seleccionados.
   c. Si el disco de destino que se asigna automáticamente es el volumen de destino correcto, seleccione **Destination Disk (Disco de destino)**.
   d. Haga clic en **Rollback (Revertir)** y, después, continúe al paso 3.
2. Para asignar volúmenes manualmente, realice estos pasos:
   a. En el cuadro de diálogo **RollbackURC**, seleccione la pestaña **Manually Map Volumes (Asignar volúmenes manualmente)**.
   b. En el área **Volume Mapping (Asignación de volúmenes)**, en **Source Volume (Volumen de origen)**, compruebe que el volumen de origen está seleccionado y que los volúmenes adecuados aparecen debajo y están seleccionados.
   c. En **Destination (Destino)**, en el menú desplegable, seleccione el destino adecuado que representará el volumen de destino para realizar la restauración desde cero del punto de recuperación seleccionado y, después, haga clic en **Rollback (Revertir)**.
3. En el cuadro de diálogo de confirmación **RollbackURC**, revise la asignación del origen del punto de recuperación y el volumen de destino de la reversión. Para realizar la reversión, haga clic en **Begin Rollback (Iniciar reversión)**.

   AVISO: Si selecciona Begin Rollback (Iniciar reversión), todas las particiones y datos de la unidad de destino se eliminarán de manera permanente, y se reemplazarán por el contenido del punto de recuperación seleccionado, incluido el sistema operativo y los datos.

Visualización del progreso de la recuperación

Para ver el progreso de la recuperación:

1. Después de iniciar el proceso de reversión, aparece el cuadro de diálogo **Active Task (Tarea activa)**, que muestra que la acción de reversión se ha iniciado.

   NOTA: La aparición del cuadro de diálogo **Active Task (Tarea activa)** no significa que la tarea se haya completado correctamente.

2. De manera opcional, puede supervisar el progreso de la tarea desde el cuadro de diálogo Active Task (Tarea activa). Para ello, haga clic en **Open Monitor Window (Abrir ventana del monitor)** y aparecerá el estado de la recuperación, así como la hora de inicio y de finalización en la ventana **Monitor Open Task (Supervisar tarea abierta)**.

   NOTA: Para volver a los puntos de recuperación de la máquina de origen, en el cuadro de diálogo **Active Task (Tarea activa)**, haga clic en **Close (Cerrar)**.

Inicio de un servidor de destino restaurado

Para iniciar un servidor de destino restaurado:

1. Vuelva al servidor de destino y, en la interfaz de la **AppAssure Universal Recovery Console (Consola de recuperación universal de AppAssure)**, haga clic en **Reboot (Reiniciar)** para iniciar la máquina.
2. Especifique que Windows se inicie normalmente.
3. Inicie la sesión en la máquina.

   El sistema se restaurará a su estado anterior a la restauración desde cero.

Reparación de problemas de inicio

Tenga en cuenta que, si va a restaurar en hardware diferente, deberá insertar una controladora de almacenamiento, un disco RAID, una interfaz AHCI, un conjunto de chips u otros controladores, en caso de que aún no estén incluidos en el CD de inicio. Estos controladores permiten que el sistema operativo funcione en todos los dispositivos del servidor de destino correctamente.

Para reparar problemas de arranque:

1. Si detecta problemas al iniciar el servidor de destino restaurado, abra la Consola de recuperación universal volviendo a cargar el CD de inicio.
2. En la Consola de recuperación universal, haga clic en **Driver Injection (Inserción de controlador)**.
3. En el cuadro de diálogo Driver Injection (Inserción de controlador), haga clic en **Repair Boot Problems (Reparar problemas de inicio)**.

   Los parámetros de inicio del registro de inicio del servidor de destino se repararán de forma automática.
4. En la Consola de recuperación universal, haga clic en **Reboot (Reiniciar)**.

Cómo realizar una restauración desde cero para una máquina Linux

Puede realizar una Bare Metal Restore (Restauración completa - BMR) de una máquina Linux que incluya una reversión del volumen del sistema. Mediante la utilidad de línea de comandos de AppAssure, `aamount`, revierta a la imagen base del volumen de inicio. Antes de realizar una BMR para una máquina Linux, primero debe hacer lo siguiente:

- Obtenga un archivo de Live CD de BMR de la asistencia de AppAssure, que incluye una versión de inicio de Linux.

  NOTA: También puede descargar el archivo de Live CD de Linux del portal de licencias, en la dirección **https://licenseportal.com**.

- Asegúrese de que hay espacio suficiente en el disco duro para crear particiones de destino en la máquina de destino que contengan los volúmenes de origen. Las particiones de destino deben tener un tamaño igual o superior a la partición de origen inicial.
- Identifique la ruta para la reversión, que será la ruta del descriptor de archivo de dispositivo. Para ello, use el comando `fdisk` desde una ventana de terminal.

  NOTA: Antes de empezar a utilizar los comandos de AppAssure, instale la utilidad de pantalla. Esta utilidad le permite desplazarse por la pantalla para ver más datos, como una lista de puntos de recuperación. Para obtener más información acerca de la instalación de la utilidad de pantalla, consulte Instalación de la utilidad de pantalla.

Para realizar una restauración desde cero para una máquina Linux:

1. Con el archivo de Live CD que reciba de AppAssure, inicie la máquina Linux y abra una ventana de terminal.
2. Si fuera necesario, cree una nueva partición de disco, por ejemplo, ejecutando el comando `fdisk` como raíz y haga que esta partición se pueda iniciar mediante el comando `a`.
3. Ejecute la utilidad `aamount` de AppAssure como raíz, por ejemplo:

   ```
   sudo aamount
   ```
4. En la solicitud de montaje de AppAssure, introduzca el siguiente comando para enumerar las máquinas protegidas:

   ```
   lm
   ```
5. Cuando se le solicite, introduzca la dirección IP o nombre del host del servidor AppAssure Core.
6. Introduzca las credenciales de inicio de sesión, es decir, el nombre de usuario y la contraseña, para este servidor.

   Aparece una lista que muestra las máquinas protegidas por este servidor AppAssure Core, y que enumera las máquinas encontradas por número de elemento de línea, dirección de host/IP y un número de Id. para la máquina (por ejemplo: `293cc667-44b4-48ab-91d8-44bc74252a4f`).
7. Para ver los puntos de recuperación montados actualmente para la máquina que desea restaurar, introduzca el siguiente comando:

   ```
   lr <machine_line_item_number>
   ```

   NOTA: También puede introducir el número de Id. de la máquina en lugar del número de elemento de línea.

   Aparece una lista que muestra los puntos de recuperación básicos e incrementales de dicha máquina. Esta lista incluye un número de elemento de línea, fecha/fecha y hora, ubicación de volumen, tamaño de punto de recuperación y un número de Id. para el volumen que incluye un número de secuencia al final (por ejemplo: "`293cc667-44b4-48ab-91d8-44bc74252a4f:2`"), que identifica el punto de recuperación.
8. Para seleccionar el punto de recuperación de la imagen base que se va a revertir, introduzca el siguiente comando:

   ```
   r <volume_base_image_recovery_point_ID_number> <path>
   ```

   PRECAUCIÓN: Asegúrese de que el volumen del sistema no esté montado.

   Este comando revierte la imagen de volumen especificada por el Id. del Core en la ruta de acceso especificada. La ruta de acceso para la reversión es la ruta de acceso para el descriptor de archivo de dispositivo y no el directorio en el que está montado.

NOTA: También puede especificar un número de línea en el comando en lugar del número de Id. de punto de recuperación para identificar el punto de recuperación. Utilice el número de línea de máquina/Agent (en la salida de lm), seguido del número de línea de punto de recuperación y de la letra de volumen, seguido de la rutade acceso, por ejemplo, `r <machine_line_item_number> <base_image_recovery_point_line_number> <volume_letter> <path>`. En este comando, `<path>`está el descriptor de archivo del volumen real.

9. Si se le solicita que continúe, escriba `y` para Sí.

   Mientras continúe la reversión, aparecerán una serie de mensajes para notificarle el estado.

10. Tras una reversión satisfactoria, actualice el registro de inicio principal con el cargador de inicio restaurado.

    NOTA: La reparación o configuración del cargador de inicio solo es necesaria si el disco es nuevo. Si se trata de una reversión simple en el mismo disco, la configuración del cargador de inicio no será necesaria.

    PRECAUCIÓN: No desmonte un volumen Linux protegido manualmente. En caso de que necesite hacerlo, ejecute el siguiente comando antes de desmontar el volumen: bsctl -d <path to volume>.

    En este comando, `<path to volume>` no se hace referencia al punto de montaje del volumen sino al descriptor de archivo del volumen;debe tener un formato similar al de este ejemplo: **/dev/sda1**.

Instalación de la utilidad de pantalla

Antes de empezar a utilizar los comandos de AppAssure, instale la utilidad de pantalla. Esta utilidad le permite desplazarse por la pantalla para ver más datos, como una lista de puntos de recuperación.

Para instalar la utilidad de pantalla:

1. Utilice el archivo de Live CD para iniciar la máquina Linux.

   Se abrirá una ventana de terminal.

2. Introduzca el siguiente comando: `sudo apt-get install screen`
3. Para iniciar la utilidad de pantalla, escriba `screen` en el símbolo del sistema.

Creación de particiones de inicio en una máquina Linux

Para crear particiones de inicio en una máquina Linux mediante la línea de comandos:

1. Conecte todos los dispositivos mediante la utilidad **bsctl** con el siguiente comando como raíz: `sudo bsctl --attach-to-device /dev/<restored volume>`

   NOTA: Repita este paso para cada volumen restaurado.

2. Utilice los siguientes comandos para montar los volúmenes restaurados:

   ```
   mount /dev/<restored volume> /mnt

   mount /dev/<restored volume> /mnt
   ```

   NOTA: Puede que algunas configuraciones del sistema incluyan el directorio de inicio como parte del volumen raíz.

3. Utilice los siguientes comandos para montar los metadatos de instantáneas de los volúmenes restaurados:

```
sudo bsctl --reset-bitmap-store /dev/<restored volume>

sudo bsctl --map-bitmap-store /dev/<restored volume>
```

4. Compruebe que el identificador único universal (UUID) contiene volúmenes nuevos mediante el comando `blkid` o `ll /dev/disk/by-uuid`.
5. Compruebe que `/etc/fstab` contiene los UUID correctos para los volúmenes raíz y de inicio.
6. Instale el cargador de arranque unificado (GRUB) mediante los siguientes comandos:

```
mount --bind /dev/ /mnt/dev

mount --bind /dev/ /mnt/dev

chroot/mnt/bin/bash

grub-install/dev/sda
```

7. Compruebe que el archivo **/boot/grub/grub.conf** contiene el UUID correcto para el volumen raíz, o actualícelo según sea necesario con un editor de texto.
8. Extraiga el disco de Live CD de la unidad de CD-ROM y reinicie la máquina Linux.

Visualización de eventos y alertas

Para ver eventos y alertas:

1. Realice uno de los siguientes pasos:
   - En la pestaña Machines (Máquinas) de la Core Console, haga clic en el hiperenlace de la máquina de la cual desea ver los eventos.
   - En el área de **Navigation (Navegación)** izquierda de la Core Console, seleccione la máquina de la cual desea ver los eventos.
2. Haga clic en la pestaña **Events (Eventos)**.

   Aparece un registro de todos los eventos para tareas y alertas actuales.

5

Protección de clústeres de servidor

Acerca de la protección de clúster de servidor

En AppAssure, la protección de clúster de servidor está asociada con el Agent de AppAssure instalado en nodos de clúster individuales (esto es, máquinas individuales en el clúster), y el Core, que protege dichos Agents, todo ello como si fueran una única máquina compuesta.

Puede fácilmente configurar un Core para proteger y administrar un clúster. En la Core Console, un clúster está organizado como entidad independiente, que actúa como "contenedor" para incluir los nodos relacionados. Por ejemplo, en el área de navegación izquierda, el Core aparece en la parte superior del árbol de navegación, y los clústeres aparecen debajo del Core y contienen los nodos individuales asociados (en los que están instalados los Agents de AppAssure).

En los niveles de Core y clúster, puede ver información sobre el clúster, como por ejemplo la lista de nodos relacionados y volúmenes compartidos. Un clúster se muetsra en la Core Console en la pestaña Machines (Máquinas) y puede cambiar la vista (con Show/Hide [Mostrar/Ocultar]) para ver los nodos incluidos en el clúster. En el nivel de clúster, también puede ver los metadatos de clúster de SQLy de Exchange correspondientes para los nodos del clúster. Puede especificar la configuración de todo el clúster y los volúmenes compartidos de dicho clúster o ir a un nodo individual (máquina) del clúster para configurar los valores solo de dicho nodo y los volúmenes locales asociados.

Aplicaciones admitidas y tipos de clúster

Para proteger su clúster correctamente, debe haber instalado el AppAssure 5 Agent en cada uno de los nodos o máquinas del clúster. AppAssure 5 admite las versiones de aplicación y las configuraciones de clúster de la siguiente tabla.

Aplicación	Versión de aplicación y configuración de clúster relacionado	Clúster de conmutación por error de Windows
Microsoft Exchange	Clúster de copia única, 2007 (SCC)	2003, 2008, 2008 R2
	Replicación continua de clúster, 2007 (CCR)	
	Grupo de disponibilidad de base de datos, 2010 (DAG)	2008, 2008 R2
Microsoft SQL	Clúster de copia única, 2005, 2008, 2008 R2 (SCC)	2003, 2008, 2008 R2
	Clúster de copia única (SCC), 2012	2008, 2008 R2, 2012

Los tipos de disco admitidos incluyen:

- Discos de Tabla de partición GUID (GPT) mayores de 2 TB
- Discos dinámicos
- Discos básicos

Algunos de los tipos de montaje admitidos:

- Unidades compartidas que se conectan como letras de unidad (por ejemplo, D:)
- Volúmenes dinámicos simples en un disco físico simple (no se admiten volúmenes seccionados, reflejados ni distribuidos)
- Unidades compartidas que se conectan como puntos de montaje

Protección de un clúster

Este tema describe cómo agregar un clúster para protección en AppAssure. Al agregar un clúster para protección, debe especificar el nombre de host o la dirección IPdel clúster, la aplicación de clúster o uno de los nodos o máquinas de clúster que incluya AppAssure 5 Agent.

NOTA: Se utiliza un repositorio para almacenar las instantáneas de datos capturadas de sus nodos protegidos. Antes de empezar a proteger datos en su clúster, configure al menos un repositorio que esté asociado con su AppAssure Core.

Para obtener información sobre la configuración de repositorios, consulte Acerca de los repositorios.

Para proteger un clúster:

1. Realice uno de los siguientes pasos:
   - En la Core Console, acceda a la pestaña **Home (Inicio)** y haga clic en el botón **Protect Cluster (Proteger clúster)**.
   - En la Core Console, en la pestaña **Machines (Máquinas)**, haga clic en **Actions (Acciones)** y, a continuación, haga clic en **Protect Cluster (Proteger clúster)**.
2. En el cuadro de diálogo **Connect to Cluster (Conectar a clúster)**, introduzca la siguiente información:

Cuadro de texto	Descripción
Host	El nombre de host o dirección IP del clúster, la aplicación de clúster o uno de los nodos de clúster que desea proteger. NOTA: Si utiliza la dirección IP de uno de los nodos, dicho nodo deberá tener instalado e iniciado un Agent de AppAssure.
Port	El número de puerto en la máquina en la que AppAssure 5 Core se comunica con el Agent.
Nombre de usuario	El nombre de usuario del administrador de dominio utilizado para conectar a esta máquina; por ejemplo, **domain_name\administrator** o **administrator@domain_name.com** NOTA: El nombre de dominio es obligatorio. No puede conectarse al clúster utilizando el nombre de dominio de administrador local.
Contraseña	La contraseña que se utiliza para conectar a esa máquina.

3. En el cuadro de diálogo **Protect Cluster (Proteger clúster)**, seleccione un repositorio para este clúster.
4. Para proteger el clúster en función de la configuración predeterminada, seleccione los nodos para la protección predeterminada y haga clic en **Protect (Proteger)**.

NOTA: La configuración predeterminada garantiza que todos los volúmenes estén protegidos con un programa predeterminado cada 60 minutos.

5. Para introducir una configuración personalizada para el clúster (por ejemplo, para personalizar el programa de protección para los volúmenes compartidos), haga lo siguiente:
   a. Haga clic en **Settings (Valores)**.
   b. En el cuadro de diálogo **Volumes (Volúmenes)**, seleccione los volúmenes para proteger y, a continuación, haga clic en **Edit (Editar)**.
   c. En el cuadro de diálogo **Protection Schedule (Programa de protección)**, seleccione una de las opciones de programa siguientes para proteger los datos como se describe en la tabla siguiente.

Cuadro de texto	Descripción
Interval (Intervalo)	Puede elegir entre: • **Weekday (Día de la semana)**:para proteger los datos en un intervalo específico, seleccione **Interval (Intervalo)** y, a continuación: – Para personalizar cuándo proteger datos durante las horas de máxima actividad, puede especificar una hora de inicio y una hora de finalización y un intervalo. – Para proteger los datos fuera del horario de máxima actividad, seleccione la casilla de verificación **Protect during off-peak times (Protección fuera del horario de máxima actividad)** y, a continuación, seleccione un intervalo para la protección. • **Weekends (Fines de semana)**: para proteger también los datos durante los fines de semana, seleccione la casilla de verificación **Protect during weekends (Proteger durante los fines de semana)** y, a continuación, seleccione un intervalo.
Daily (Diariamente)	Para proteger los datos diariamente, seleccione la opción **Daily** (Diario) y, a continuación, en **Protection Time (Hora de la protección)** seleccione la hora para iniciar la protección de los datos.
No Protection (Sin protección)	Para eliminar la protección de este volumen, seleccione la opción **No Protection (Sin protección)**.

6. Cuando haya hecho todos los cambios necesarios, haga clic en **Save (Guardar)**.
7. Para introducir la configuración personalizada para un nodo del clúster, seleccione un nodo y, a continuación, haga clic en el enlace **Settings (Valores)** situado al lado del nodo.
   • Repita el paso 5 para editar el programa de protección.

   Para obtener más información sobre cómo personalizar nodos, consulte Protección de nodos en un clúster.
8. En el cuadro de diálogo **Protect Cluster (Proteger clúster)**, haga clic en **Protect (Proteger)**.

Protección de nodos en un clúster

Este tema describe cómo proteger los datos de una máquina o nodo de clúster que tenga un Agent de AppAssure instalado. Al agregar protección, deberá seleccionar un nodo de la lista de nodos disponibles, así como especificar el nombre de host y el nombre de usuario y la contraseña del administrador del dominio.

Para proteger los nodos de un clúster:

1. Después de agregar un clúster, vaya a dicho clúster y haga clic en la pestaña **Machines (Máquinas)**.
2. Haga clic en el menú **Actions (Acciones)** y, a continuación, haga clic en **Protect Cluster Node (Proteger nodo de clústeres)**.
3. En el cuadro de diálogo **Protect Cluster Node (Proteger nodo de clústeres)**, seleccione o introduzca la información siguiente según corresponda y, a continuación, haga clic en **Connect (Conectar)** para agregar la máquina o el nodo.

Cuadro de texto	Descripción
Host	Una lista desplegable de nodos en el clúster disponibles para protección.
Port	El número de puerto por el que el Core se comunica con el Agent en el nodo.
Nombre de usuario	El nombre de usuario del administrador de dominio utilizado para conectarse a este nodo. Por ejemplo, **example_domain\administrator** para **administrator@example_domain.com**.
Contraseña	La contraseña que se utiliza para conectar a esa máquina.

4. Haga clic en **Protect (Proteger)** para iniciar la protección de esta máquina con la configuración de protección predeterminada.

   NOTA: La configuración predeterminada garantiza que todos los volúmenes de esta máquina estén protegidos con un programa predeterminado cada 60 minutos.

5. Para introducir la configuración personalizada para esta máquina, (por ejemplo, para cambiar el nombre de visualización), añadir cifrado o personalizar el programa de protección), haga clic en **Show Advanced Options (Mostrar opciones avanzadas)**.
6. Edite los siguientes valores según sea necesario, tal como se describe a continuación.

Cuadro de texto	Descripción
Nombre de visualización	Introduzca el nuevo nombre de la máquina que aparecerá en la Core Console.
Repository (Repositorio)	Seleccione el repositorio en el Core donde se almacenarán los datos de esta máquina.
Cifrado	Especifique si el cifrado debe aplicarse a los datos de cada volumen de esta máquina que se almacenarán en el repositorio. NOTA: La configuración del cifrado de un repositorio se define en la pestaña **Configuration (Configuración)** de la Core Console.
Programa	Seleccione una de las opciones siguientes. • Protect all volumes with default schedule (Proteger todos los volúmenes con el programa predeterminado). • Protect specific volumes with custom schedule (Proteger volúmenes específicos con programa personalizado). A continuación, en **Volumes (Volúmenes)**, elija un volumen y haga clic en **Edit (Editar)**. Para obtener más información acerca de cómo establecer intervalos personalizados, consulte Cómo proteger un clúster.

Proceso de modificación de la configuración del nodo de clúster

Una vez que haya agregado protección para nodos de clúster, puede fácilmente modificar los valores de configuración básicos para esas máquinas o nodos (por ejemplo, nombre de visualización, nombre de host, etc.), la configuración de la protección (por ejemplo, cambiar el programa de protección para volúmenes en la máquina, agregar o eliminar volúmenes y pausar la protección), etc.

Para modificar la configuración del nodo de clúster, debe realizar las tareas siguientes:

1. Realice uno de los siguientes pasos:
   - Vaya hasta el clúster que contiene el nodo que desee modificar, haga clic en la pestaña **Machines (Máquinas)**, y seleccione la máquina o el nodo que desee modificar.
   - O, en el panel **Navigation (Navegación)**, bajo el encabezado **Cluster (Clúster)**, seleccione la máquina o el nodo que desee modificar.
2. Para modificar y ver los valores de configuración, consulte Visualización y modificación de valores de configuración.
3. Para configurar los grupos de notificación para eventos del sistema, consulte Configuring Notification Groups For System Events(Configuración de grupos de notificación para eventos del sistema).
4. Para personalizar la configuración de la política de retención, consulte Personalización de la configuración de la política de retención.
5. Para modificar el programa de protección, consulte Modificación de los programas de protección.
6. Para modificar la configuración de la transferencia, consulte Modificación de la configuración de las transferencias.

Plan para configurar los valores del clúster

El plan para configurar los valores del clúster implica realizar las siguientes tareas:

- Modificación de la configuración de clúster
- Configuración de notificaciones de evento de clúster
- Modificación de la política de retención de clústeres
- Modificación de los programas de protección de clúster
- Modificación de la configuración de transferencia de clúster

Modificación de la configuración de clúster

Después de agregar un clúster, puede modificar con facilidad valores básicos (por ejemplo, el nombre de visualización), valores de protección (por ejemplo, programas de protección, agregar o quitar volúmenes y pausar la protección), etc.

Para modificar la configuración de clúster:

1. Realice uno de los siguientes pasos:
   - En la Core Console, haga clic en la pestaña **Machines (Máquinas)** y, a continuación, seleccione el clúster que desee modificar.
   - En el área de navegación izquierda, seleccione el clúster que desee modificar.
2. Haga clic en la pestaña **Configuration (Configuración)**.

   Aparecerá la página **Settings (Valores)**.

3. Haga clic en **Edit (Editar)** para modificar la configuración de esta página para el clúster según se describe a continuación.

Cuadro de texto	Descripción
Nombre de visualización	Introduzca el nombre de visualización del clúster. El nombre para este clúster se muestra en la Core Console. De manera predeterminada, este es el nombre del host del clúster. Puede cambiarlo por un nombre más descriptivo si lo desea.
Nombre del host	Este valor representa el nombre del host para el clúster. Se muestra aquí solo por fines informativos y no se puede modificar.
Repository (Repositorio)	Especifique el repositorio de Core asociado al clúster. NOTA: Si ya se han tomado instantáneas para este clúster, esta configuración se muestra aquí solo por información y no se puede modificar.
Encryption Key (Clave de cifrado)	Edite y seleccione una clave de cifrado, si fuera necesario. Especifica si el cifrado debe aplicarse a los datos de cada volumen de este clúster que se almacenarán en el repositorio.

Configuración de notificaciones de evento de clúster

Puede configurar cómo se informa de los eventos del sistema para su clúster al crear grupos de notificación. Estos eventos podrían ser alertas del sistema o errores.

Para configurar notificaciones de eventos de clúster

1. Realice uno de los siguientes pasos:
   - En la Core Console, haga clic en la pestaña **Machines (Máquinas)** y, a continuación, seleccione el clúster que desee modificar.
   - En el área de navegación izquierda, seleccione el clúster que desee modificar.
2. Seleccione la pestaña **Configuration (Configuración)** y, a continuación, haga clic en **Events (Eventos)**.
3. Seleccione una de las opciones descritas en la siguiente tabla.

Cuadro de texto	Descripción
Use Core alert settings (Utilizar la configuración de alerta del Core)	Esto adopta la configuración que usa el Core asociado: a. Haga clic en **Apply (Aplicar)**. b. Complete el paso 5.
Use Custom alert settings (Utilizar configuración de alertas personalizada)	Le permite configurar valores personalizados. Continúe con el paso 4.

4. Si selecciona **Custom alert settings (Configuración de alertas personalizada)**, haga clic en **Add Group (Agregar grupo)** para agregar un grupo de notificación nuevo para enviar una lista de eventos del sistema.

Se abre el cuadro de diálogo **Add Notification Group (Agregar grupo de notificación)**.

5. Agregue las opciones de notificación según se describe en la tabla siguiente.

Cuadro de texto	Descripción
Nombre	Introduzca un nombre para el grupo de notificación.
Descripción	Introduzca una descripción del grupo de notificación.
Enable Events (Habilitar eventos)	Seleccione los eventos a notificar, por ejemplo, Clusteres (Clústeres). También puede elegir la selección por tipo: • **Error** • **Aviso** • **Informativa** NOTA: Si elige seleccionar por tipo, de manera predeterminada, los eventos correspondientes se habilitarán de forma automática. Por ejemplo, si elige Warning(Aviso), se habilitarán los eventos Attachability, Jobs, Licensing, Archive, CoreService, Export, Protection, Replication y Rollback.
Notification Options (Opciones de notificación)	Seleccione el método para especificar cómo administrar notificaciones. Puede elegir entre las siguientes opciones: • **Notify by Email (Notificar por correo electrónico**: especifique a qué direcciones de correo electrónico enviar los eventos en los campos To (Para), CC y BCC (CCO). • **Notify by Windows Event log (Notificar por registro de eventos de Windows)**:el registro de eventos de Windows controla la notificación. • **Notify by syslogd (Notificar por syslogd)**: especifique a qué nombre del host y puerto enviar los eventos.

6. Haga clic en **OK (Aceptar)** para guardar sus cambios y, a continuación, haga clic en **Apply (Aplicar)**.
7. Para editar un grupo de notificación existente, junto al grupo de notificación en la lista haga clic en **Edit (Editar)**.

   Se abrirá el cuadro de diálogo **Edit Notification Group (Editar grupo de notificación)** para que pueda editar la configuración.

Modificación de la política de retención de clúster

La política de retención de un clúster especifica el tiempo que se almacenan en el repositorio los puntos de recuperación para los volúmenes compartidos en el clúster. Las políticas de retención se utilizan para conservar instantáneas de copia de seguridad durante períodos de tiempo más largos y para ayudar con la administración de estas instantáneas de copia de seguridad. La política de retención la aplica un proceso de mantenimiento periódico que ayuda a envejecer y eliminar copias de seguridad viejas.

1. Realice uno de los siguientes pasos:
   - En la **Core Console**, haga clic en la pestaña **Machines (Máquinas)** y, a continuación, seleccione el clúster que desee modificar.
   - En el área de navegación izquierda, seleccione el clúster que desee modificar.
2. Seleccione la pestaña **Configuration (Configuración)** y, a continuación, haga clic en **Retention Policy (Política de retención)**.
3. Seleccione una de las opciones de la siguiente tabla.

Cuadro de texto	Descripción
Use Core default retention policy (Utilizar la política de retención predeterminada del Core)	Esto adopta la configuración que usa el Core asociado. Haga clic en **Apply (Aplicar)**.
Use Custom retention policy (Utilizar la política de retención personalizada)	Le permite configurar valores personalizados.

NOTA: Si ha seleccionado **Custom alert settings (Configuración de alertas personalizadas)**, siga las instrucciones para configurar una política de retención personalizada según se describe en Cómo personalizar la configuración de la política de retención, empezando por el paso 4.

Modificación de los programas de protección de clúster

Puede modificar los programas de protección solo si su clúster tiene volúmenes compartidos.

Para modificar los programas de protección de clúster:

1. Realice uno de los siguientes pasos:
   - En la Core Console, haga clic en la pestaña **Machines (Máquinas)** y, a continuación, seleccione el clúster que desee modificar.
   - En el área de navegación izquierda, seleccione el clúster que desee modificar.
2. Haga clic en la pestaña **Configuration (Configuración)** y, a continuación, haga clic en **Protection Settings (Configuración de la protección)**.
3. Siga las instrucciones para modificar la configuración de protección, según se describe en Cómo modificar los programas de protección, empezando por el paso 2.

Modificación de la configuración de transferencia de clúster

En AppAssure 5, puede modificar fácilmente la configuración para administrar los procesos de transferencia de datos de un clúster protegido.

NOTA: Podrá modificar la configuración de transferencia de clúster solo si éste tiene volúmenes compartidos.

Hay tres tipos de transferencias en AppAssure 5:

Cuadro de texto	Descripción
Instantáneas	Se realiza una copia de seguridad de los datos del clúster protegido.
Exportación de la VM	Se crea una máquina virtual con toda la información de copia de seguridad y los parámetros según lo especificado en el programa definido para la protección del clúster.
Rollback	Se restaura la información de copia de seguridad para un clúster protegido.

Para modificar la configuración de transferencia de clúster:

1. Realice uno de los siguientes pasos:

- En la Core Console, haga clic en la pestaña **Machines (Máquinas)** y, a continuación, seleccione el clúster que desee modificar.
- En el área de navegación izquierda, seleccione el clúster que desee modificar.

2. Haga clic en la pestaña **Configuration (Configuración)** y, a continuación, haga clic en **Transfer Settings (Configuración de transferencia)**.
3. Modifique la configuración de protección según se describe en Modificación de los programas de protección, comenzando por el paso 2.

Conversión de un nodo de clúster protegido en un Agent

En AppAssure 5, puede convertir un nodo de clúster protegido en un AppAssure Agent de manera que el Core pueda continuar administrándolo, aunque ya no forme parte del clúster. Esto es útil, por ejemplo, si necesita quitar el nodo de clúster del propio clúster, pero aún desea mantener su protección.

Para convertir un nodo de clúster protegido en un Agent:

1. Realice uno de los siguientes pasos:
   - En la Core Console, haga clic en la pestaña **Machines (Máquinas)**, y seleccione el clúster que contiene la máquina que desea convertir. A continuación, haga clic en la pestaña **Machines (Máquinas)** para el clúster.
   - En el área de navegación izquierda, seleccione el clúster que contiene la máquina que desea convertir y haga clic en la pestaña **Machines (Máquinas)**.
2. Seleccione la máquina para convertir y, a continuación, en el menú desplegable haga clic en **Actions (Acciones)** en la parte superior de la pestaña Machines (Máquinas) y haga clic en **Convert to Agent (Convertir en Agent)**.
3. Para agregar la máquina nuevamente al clúster, selecciónela y, a continuación, haga clic en la pestaña **Summary (Resumen)**, en el menú **Actions (Acciones)** y en **Convert to Node (Convertir en nodo)**.

Visualización de información del clúster del servidor

Visualización de información del sistema de clúster

Para ver la información del sistema del clúster:

1. Realice uno de los siguientes pasos:
   - En la Core Console, haga clic en la pestaña **Machines (Máquinas)** y, a continuación, seleccione el clúster que desee ver.
   - En el área **Navigation (Navegación)** izquierda, seleccione el clúster que desee ver.
2. Haga clic en la pestaña **Tools (Herramientas)**.

   Se muestra la página **System Information (Información del sistema)** con detalles del sistema sobre el clúster, como el nombre, nodos incluidos con el estado asociado y las versiones de Windows, información de interfaz de red e información de capacidad del volumen.

Visualización de eventos y alertas del clúster

Para obtener información sobre la visualización de eventos y alertas de una máquina o un nodo individual en un clúster, consulte Visualización de eventos y alertas.

Para ver eventos y alertas del clúster:

1. Realice uno de los siguientes pasos:
   - En la Core Console, haga clic en la pestaña **Machines (Máquinas)** y, a continuación, seleccione el clúster que desee ver.

- En el área de **Navigation (Navegación)** izquierda, bajo **Clusters (Clústeres)**, seleccione el clúster que desee ver.

2. Haga clic en la pestaña **Events (Eventos)**.

   Un registro muestra todos los eventos para las tareas actuales, así como cualquier alerta para el clúster.

3. Para filtrar la lista de eventos, puede seleccionar o borrar la verificación de las casillas **Active (Activo)**, **Complete (Completo)** o **Failed (En error)**, según corresponda
4. En la tabla **Alerts (Alertas)**, haga clic en **Dismiss All (Descartar todo)** para descartar todas las alertas de la lista.

Visualización de la información de resumen

Para ver la información de resumen:

1. Realice uno de los siguientes pasos:
   - En la Core Console, haga clic en la pestaña **Machines (Máquinas)** y, a continuación, seleccione el clúster que desee ver.
   - En el área de **Navigation (Navegación)** izquierda, bajo **Clusters (Clústeres)**, seleccione el clúster que desee ver.
2. En la pestaña **Summary (Resumen)**, puede ver información como el nombre del clúster, tipo de clúster, tipo de quórum (si corresponde) y ruta de acceso de quórum (si corresponde).

   En esta pestaña también se muestra información de un vistazo sobre los volúmenes de este clúster, que incluye el tamaño y el programa de protección.

3. Para actualizar esta información, haga clic en el menú desplegable **Actions (Acciones)** y haga clic en **Refresh Metadata (Actualizar metadatos)**.

   Para obtener información sobre la visualización de información de resumen y estado para una máquina o nodo individual del clúster, consulte Visualización del estado de la máquina y otros detalles.

Cómo trabajar con puntos de recuperación de clúster

Un punto de recuperación, también conocido como instantánea, es una copia puntual de las carpetas y los archivos de los volúmenes compartidos de un clúster, que se almacena en el repositorio. Los puntos de recuperación se utilizan para recuperar máquinas protegidas o para montarlos en un sistema de archivos local. En AppAssure 5, puede ver las listas de puntos de recuperación en el repositorio. Lleve a cabo los pasos del siguiente procedimiento para revisar los puntos de recuperación.

NOTA: Si está protegiendo datos de un clúster de servidor DAG o CCR, los puntos de recuperación asociados no aparecerán en el nivel de clúster. Solo estarán visibles en el nivel de nodo o de máquina.

Para obtener información sobre la visualización de puntos de recuperación para máquinas individuales de un clúster, consulte Visualización de los puntos de recuperación.

Para trabajar con puntos de recuperación de clúster:

1. Realice uno de los siguientes pasos:
   - En la Core Console, haga clic en la pestaña **Machines (Máquinas)** y, a continuación, seleccione el clúster para el que desee ver puntos de recuperación.
   - En el área de navegación izquierda, bajo **Clusters (Clústeres)**, seleccione el clúster para el que desee ver los puntos de recuperación.
2. Haga clic en la pestaña **Recovery Points (Puntos de recuperación)**.
3. Para ver información detallada sobre un punto de recuperación específico, haga clic en **>** junto al punto de recuperación de la lista para ampliar la vista.

Para obtener información sobre las operaciones que puede realizar en los puntos de recuperación, consulte Visualización de un punto de recuperación específico.

4. Seleccione un punto de recuperación que montar.

   Para obtener más información sobre cómo montar un punto de recuperación, consulte Montaje de un punto de recuperación para una máquina Windows, empezando por el paso 2.

5. Para eliminar puntos de recuperación, consulte Eliminación de puntos de recuperación.

Administración de instantáneas para un clúster

Puede administrar instantáneas al forzar una instantánea o pausar las instantáneas actuales. Forzar una instantánea le permite forzar una transferencia de datos para el clúster protegido actual. Cuando se fuerza una instantánea, la transferencia se inicia inmediatamente o se agrega a la cola. Solo se transfieren los datos que hayan cambiado desde un punto de recuperación anterior. Si no existe ningún punto de recuperación anterior, se transfieren todos los datos (la imagen base) en los volúmenes protegidos. Cuando se hace una pausa en una instantánea, se detienen temporalmente todas las transferencias de datos desde la máquina actual.

Para obtener más información sobre cómo forzar instantáneas para máquinas individuales en un clúster, consulte Cómo forzar una instantánea. Para obtener más información sobre cómo pausar y reanudar instantáneas para las máquinas individuales en un clúster, ver Cómo pausar y reanudar la protección.

Cómo forzar una instantánea para un clúster

Para forzar una instantánea para un clúster:

1. Realice uno de los siguientes pasos:
   - En la Core Console, haga clic en la pestaña **Machines (Máquinas)** y, a continuación, seleccione el clúster para el que desee ver puntos de recuperación.
   - En el área de navegación izquierda, bajo **Clusters (Clústeres)**, seleccione el clúster para el que desee ver los puntos de recuperación.
2. En la pestaña **Summary (Resumen)**, haga clic en el menú desplegable **Actions (acciones)** y, a continuación, haga clic en **Force Snapshot (Forzar instantánea)**.

Cómo pausar y reanudar instantáneas de clúster

Para pausar y reanudar las instantáneas de clúster:

1. Realice uno de los siguientes pasos:
   - En la Core Console, haga clic en la pestaña **Machines (Máquinas)** y, a continuación, seleccione el clúster para el que desee ver puntos de recuperación.
   - En el área de navegación izquierda, bajo **Clusters (Clústeres)**, seleccione el clúster para el que desee ver los puntos de recuperación.
2. En la pestaña **Summary (Resumen)**, haga clic en el menú desplegable Actions (acciones) y, a continuación, haga clic en **Pause Snapshots (Pausar instantáneas)**.
3. En el cuadro de diálogo **Pause Protection (Pausar protección)**, seleccione una de las opciones descritas a continuación.

Cuadro de texto	Descripción
Pause until resumed (Pausar hasta reanudación)	Pausa la instantánea hasta que reanude manualmente la protección. Para reanudar la protección, haga clic en el menú **Actions (Acciones)** y, a continuación, haga clic en **Resume (Reanudar)**.
Pause for (Pausar durante)	Le permite especificar un tiempo en días, horas y minutos para pausar instantáneas.

Cómo desmontar puntos de recuperación locales

Para desmontar puntos de recuperación locales:

1. Realice uno de los siguientes pasos:
   - En la Core Console, haga clic en la pestaña **Machines (Máquinas)** y, a continuación, seleccione el clúster para el que desee desmontar puntos de recuperación.
   - En el área de navegación izquierda, seleccione el clúster para el que desee desmontar puntos de recuperación.
2. En la pestaña **Tools (Herramientas)**, bajo el menú **Tools (Herramientas)**, haga clic en **Mounts (Montajes)**.
3. En la lista de montajes locales, realice una de las acciones siguientes:
   - Para desmontar un montaje local individual, localice y seleccione el montaje del punto de recuperación que desee desmontar y, a continuación, haga clic en **Dismount (Desmontar)**.
   - Para desmontar todos los montajes locales, haga clic en el botón **Dismount All (Desmontar todo)**.

Como realizar una reversión para clústeres y nodos de clúster

Una reversión es el proceso de restauración de los volúmenes en una máquina desde puntos de recuperación. Para un clúster de servidor, se realiza una reversión a nivel de nodo o de máquina. Esta sección proporciona directrices para realizar una reversión para volúmenes de clúster.

Cómo realizar una reversión para clústeres CCR (Exchange) y DAG

Para realizar una reversión para clústeres SCC (Exchange, SQL):

1. Apague todos los nodos excepto uno.
2. Realice una reversión utilizando el procedimiento estándar de AppAssure para la máquina, según se describe en Cómo realizar una reversión y Cómo realizar una reversión para una máquina Linux mediante la línea de comandos.
3. Una vez terminada la reversión, monte todas las bases de datos a partir de los volúmenes de clúster.
4. Encienda el resto de nodos.
5. Para Exchange, acceda a la Exchange Management Console (Consola de administración de Exchange) y, para cada base de datos, realice la operación **Update Database Copy (Actualizar copia de base de datos)**.

Cómo realizar una reversión para clústeres SCC (Exchange, SQL)

Para realizar una reversión para clústeres SCC (Exchange, SQL):

1. Apague todos los nodos excepto uno.
2. Realice una reversión utilizando el procedimiento estándar de AppAssure de la máquina, según se describe en Cómo realizar una reversión y Cómo realizar una reversión para una máquina Linux mediante la línea de comandos.
3. Una vez terminada la reversión, monte todas las bases de datos a partir de los volúmenes de clúster.
4. Encienda el resto de nodos, de uno en uno.

   NOTA: No es necesario revertir el disco de quórum. Puede regenerarse automáticamente o mediante la función de servicio de clúster.

Replicación de datos de clúster

Cuando replique datos de un clúster, la replicación se configura en el nivel de la máquina para las máquinas individuales de dicho clúster. También puede configurar la replicación para replicar los puntos de recuperación de los volúmenes compartidos. Por ejemplo, si tiene cinco Agents que desea replicar del origen al destino.

Para obtener más información e instrucciones sobre la replicación de datos, consulte Replicación de los datos de Agent en una máquina.

Eliminación de un clúster de la protección

Para quitar un clúster de la protección:

1. Realice uno de los siguientes pasos:
   - En la Core Console, haga clic en la pestaña **Machines (Máquinas)** y, a continuación, seleccione el clúster que desee quitar.
   - En el área de navegación izquierda, seleccione el clúster que desee quitar para ver la pestaña **Summary (Resumen)**.
2. Haga clic en el menú desplegable **Actions (Acciones)** y, a continuación, haga clic en **Remove Machine (Quitar máquina)**.
3. Seleccione una de las opciones siguientes.

Opción	Descripción
Keep Recovery Points (Conservar puntos de recuperación)	Para mantener todos los puntos de recuperación actualmente almacenados para este clúster.
Remove Recovery Points (Quitar puntos de recuperación)	Para quitar del repositorio todos los puntos de recuperación actualmente almacenados para este clúster.

Eliminación de nodos de clúster de la protección

Complete los pasos en los siguientes procedimientos para eliminar nodos de clúster de la protección. Si solo desea eliminar un nodo del clúster, consulte Conversión de un nodo de clúster protegido a un Agent. Para eliminar un nodo de clúster de la protección.

1. Realice uno de los siguientes pasos:
   - En la Core Console, haga clic en la pestaña **Machines (Máquinas)**, y a continuación seleccione el clúster que contiene el nodo que desee quitar. En la pestaña **Machines (Máquinas)** para el clúster, seleccione el nodo que desee quitar.
   - En el área de navegación izquierda, bajo el clúster relacionado, seleccione el nodo que desea quitar.
2. Haga clic en el menú desplegable **Actions (Acciones)** y, a continuación, haga clic en **Remove Machine (Quitar máquina)**.
3. Seleccione una de las opciones descritas en la siguiente tabla.

Opción	Descripción
Relationship Only (Sólo relación)	Elimina el Core de origen de la replicación pero mantiene los puntos de recuperación replicados.
With Recovery Points (Con puntos de recuperación)	Elimina el Core de origen de la replicación y elimina todos los puntos de recuperación replicados de dicha máquina.

Eliminación de todos los nodos de un clúster de la protección

Para quitar todos los nodos del clúster de la protección:

1. Realice uno de los siguientes pasos:
   - En la Core Console, haga clic en la pestaña **Machines (Máquinas)** y seleccione el clúster que contiene los nodos que desee eliminar. A continuación, haga clic en la pestaña **Machines (Máquinas)** del clúster.
   - En el área de navegación izquierda, seleccione el clúster que contiene los nodos que desee quitar y, a continuación, haga clic en la pestaña **Machines (Máquinas)**.
2. Haga clic en el menú desplegable **Actions (Acciones)** en la parte superior de la pestaña **Machines (Máquinas)** y, a continuación, haga clic en **Remove Machines (Quitar máquinas)**.
3. Seleccione una de las opciones descritas en la siguiente tabla.

Opción	Descripción
Relationship Only (Sólo relación)	Elimina el Core de origen de la replicación pero mantiene los puntos de recuperación replicados.
With Recovery Points (Con puntos de recuperación)	Elimina el Core de origen de la replicación y elimina todos los puntos de recuperación replicados de dicha máquina.

Visualización de un informe de clúster o nodo

Puede crear y ver informes de errores y cumplimiento sobre las actividades de AppAssure para su clúster y nodos individuales. Los informes incluyen información de actividad de AppAssure sobre el clúster, el

nodo y los volúmenes compartidos. Para obtener más información sobre informes de AppAssure, consulte Acerca de los informes.

Para obtener más información sobre cómo exportar e imprimir opciones ubicadas en la barra de herramientas de los informes, consulte Acerca de la barra de herramientas de los informes.

Para ver un informe de clúster o nodo:

1. Realice uno de los siguientes pasos:
   - En la Core Console, haga clic en la pestaña **Machines (Máquinas)** y, a continuación seleccione un clúster para el que desee crear el informe.
   - En el área de **Navigation (Navegación)** izquierda, seleccione el clúster para el que desee crear un informe.
2. Haga clic en la pestaña **Tools (Herramientas)** y, bajo el menú **Reports (Informes)**, seleccione una de las siguientes opciones:
   - **Informe de cumplimiento**
   - **Errors Report (Informe de errores)**
3. En el calendario desplegable **Start Time (Hora de inicio)**, seleccione una fecha de inicio y, a continuación, introduzca una hora de inicio para el informe.

   NOTA: No habrá datos disponibles antes de la hora en que se implementó AppAssure 5 Core o el Agent.
4. En el calendario desplegable **End Time (Hora de finalización)**, seleccione una fecha de finalización y, a continuación, introduzca la hora de finalización para el informe.
5. Haga clic en **Generate Report (Generar informe)**.

   Si el informe ocupa varias páginas, puede hacer clic en los números de página o botones de flechas en la parte superior de los resultados del informe para ver las páginas de resultados.

   Los resultados del informe aparecen en la página.
6. Para exportar los resultados del informe en uno de los formatos disponibles(PDF, XLS, XLSX, RTF, MHT, HTML, TXT, CSV o imagen), seleccione el formato de exportación en la lista desplegable y, a continuación, lleve a cabo una de las siguientes opciones:
   - Haga clic en el primer icono **Save (Guardar)** para exportar un informe y guardarlo en el disco.
   - Haga clic en el segundo icono **Save (Guardar)** para exportar un informe y mostrarlo en una nueva ventana del explorador de web.
7. Para imprimir los resultados del informe, realice una de las acciones siguientes:
   - Haga clic en el primer icono **Printer (Impresora)** para imprimir el informe completo.
   - Haga clic en el segundo icono **Printer (Impresora)** para imprimir la página actual del informe.

6

Emisión de informes

Acerca de los informes

Su appliance DL le permite generar y ver información de resumen, de cumplimiento y de errores para varias máquinas Core y Agent.

Podrá elegir entre ver informes en línea, imprimir informes o exportarlos y guardarlos en uno de los diversos formatos admitidos. Los formatos entre los que puede elegir son:

- PDF
- XLS
- XLSX
- RTF
- MHT
- HTML
- TXT
- CSV
- Imagen

Acerca de la barra de herramientas de informes

La barra de herramientas para todos los informes le permite imprimir y guardar de dos maneras diferentes. La siguiente tabla describe las opciones para imprimir y guardar.

Icono	Descripción
	Imprimir el informe
	Imprimir la página actual
	Exportar un informe y guardarlo en el disco
	Exportar un informe y mostrarlo en una nueva ventana Utilice esta opción para copiar, pegar y enviar por correo electrónico la URL para que otros vean el informe con un explorador de web.

Acerca de los informes de cumplimiento

Los informes de cumplimiento están disponibles para el Core y AppAssure Agent. Le proporcionan una forma de ver el estado de los trabajos realizados por un determinado Core o Agent. Los trabajos fallidos aparecen en texto rojo. La información del informe de cumplimiento de Core que no esté asociada con un Agent aparece en blanco.

Los detalles sobre los trabajos se presentan en una vista de columnas que incluye las categorías siguientes:

- Core
- Agent protegido
- Tipo
- Resumen
- Estado
- Error
- Hora de inicio
- Hora de finalización
- Hora
- Trabajo total

Acerca de los informes de errores

Los informes de errores son subconjuntos de los informes de cumplimiento y están disponibles para los Cores y AppAssure Agents. Los informes de errores incluyen solo trabajos fallidos en informes de cumplimiento y los compilan en un único informe que se puede imprimir y exportar.

Los detalles sobre los errores se presentan en una vista de columnas, con las siguientes categorías:

- Core
- Agent
- Tipo
- Resumen
- Error
- Hora de inicio
- Hora de finalización
- Tiempo transcurrido
- Trabajo total

.

Acerca del informe de resumen del Core

El **Core Summary Report (Informe de resumen del Core)** incluye información sobre los repositorios del Core seleccionado y sobre los Agents protegidos por dicho Core. La información aparece como dos resúmenes en un informe.

Resumen de repositorios

La parte **Repositories (Repositorios)** del informe **Core Summary Report (Informe de resumen del Core)** incluye datos para los repositorios ubicados en el Core seleccionado. Los detalles sobre los repositorios se presentan en una vista de columnas con las siguientes categorías:

- Name (Nombre)
- Data Path (Ruta de acceso datos)
- Metadata Path (Ruta de acceso a metadatos)

- Allocated Space (Espacio asignado)
- Used Space (Espacio utilizado)
- Free Space (Espacio libre)
- Compression/Dedupe Ratio (Relación compresión/desdup.)

Resumen de Agents

La parte **Agents** del **Core Summary Report (Informe de resumen del Core)** incluye datos para todos los Agents protegidos por el Core seleccionado.

Los detalles sobre los Agents se presentan en vista de columnas, con las categorías siguientes:

- Name (Nombre)
- Protected Volumes (Volúmenes protegidos)
- Total protected space (Espacio total protegido)
- Current protected space (Espacio actual protegido)
- Change rate per day (**Average**, **Median**) (Velocidad de cambio por día [Promedio, Mediana])
- Jobs Statistic (**Passed**, **Failed**, **Canceled**) (Estadísticas de trabajos (Aprobado, Erróneo, Cancelado)

Cómo generar un informe para un Core o Agent

Para generar un informe para un Core o Agent:

1. Vaya a la Core Console y seleccione el Core o Agent para el que desee ejecutar el informe.
2. Haga clic en la pestaña **Tools (Herramientas)**.
3. En la pestaña **Tools (Herramientas)**, expanda **Reports (Informes)** en el área de navegación izquierda.
4. En el área de navegación, seleccione el informe que desee ejecutar. Los informes disponibles varían en función de la selección realizada en el paso 1 y se describen a continuación.

Máquina	Informes disponibles
Core	Informe de cumplimiento
	Informe de resumen
	Informe de errores
Agent	Informe de cumplimiento
	Informe de errores

5. En el calendario desplegable **Start Time (Hora de inicio)**, seleccione una fecha de inicio y, a continuación, introduzca una hora de inicio para el informe.

   NOTA: No hay datos disponibles anteriores a la creación del Core o Agent.
6. En el calendario desplegable **End Time (Hora de finalización)**, seleccione una fecha de finalización y, a continuación, introduzca la hora de finalización para el informe.
7. Para un **Core Summary Report (Informe de resumen del Core)**, seleccione la casilla de verificación **All Time (Todo el tiempo)** si desea que la **Start Time (Hora de inicio)** y la **End Time (Hora de finalización)** abarquen toda la vida útil del Core.
8. Para un **Core Compliance Report (Informe de cumplimiento del Core)** o un **Core Errors Report (Informe de errores del Core)**, utilice la lista desplegable **Target Cores (Cores de destino)** para seleccionar el Core para el que desee ver datos.

9. Haga clic en **Generate Report (Generar informe)**.

   Una vez que se haya generado el informe, puede usar la barra de herramientas para imprimirlo o exportarlo.

Acerca de los informes de Core de la Central Management Console (Consola de administración central)

Su appliance DL le permite generar y ver información de resumen, de cumplimiento y de errores de varios Cores. Los detalles sobre los Cores se presentan en vistas de columna con las mismas categorías descritas en esta sección.

Cómo generar un informe desde la Central Management Console (Consola de administración central)

Para generar un informe desde la Central Management Console (Consola de administración central):

1. En la pantalla **Central Management Console Welcome (Bienvenido a la Consola de administración central)**, haga clic en el menú desplegable en la esquina superior derecha.
2. En el menú desplegable, haga clic en **Reports (Informes)** y, a continuación, seleccione una de las siguientes opciones:
   - **Informe de cumplimiento**
   - **Informe de resumen**
   - **Informe de errores**
3. En el área de navegación izquierda, seleccione el Core o los Cores para los que desee ejecutar el informe.
4. En el calendario desplegable **Start Time (Hora de inicio)**, seleccione una fecha de inicio y, a continuación, introduzca una hora de inicio para el informe.

   NOTA: No hay datos disponibles antes del momento en el que se implementaron los Cores.
5. En el calendario desplegable **End Time (Hora de finalización)**, seleccione una fecha de finalización y, a continuación, introduzca la hora de finalización para el informe.
6. Haga clic en **Generate Report (Generar informe)**.

   Una vez que se haya generado el informe, puede usar la barra de herramientas para imprimirlo o exportarlo.

7

Realizar una recuperación completa del appliance DL4000

Las unidades de datos del DL4000 Backup To Disk appliance (Appliance de copia de seguridad en disco DL4000) se ubican en las ranuras 2-9 y están en formato RAID 6, lo que indica que pueden aguantar hasta dos errores de unidad sin pérdida de datos. El sistema operativo reside en las unidades 0 y 1, que están formateadas como un disco virtual RAID 1. Si fallan estos dos discos, deberá reemplazar las unidades y reinstalar el software necesario para que el servidor vuelva a funcionar de nuevo. Para realizar una recuperación completa del servidor, debe:

- Crear una partición RAID 1 para el sistema operativo
- Instalar el sistema operativo
- Ejecutar la Recovery and Update Utility (Utilidad de recuperación y actualización)
- Volver a montar los volúmenes

Creación de una partición RAID 1 para el sistema operativo

PRECAUCIÓN: Es importante realizar estas operaciones solo en los discos virtuales RAID 1 que contienen el sistema operativo. No realice estas operaciones en los discos virtuales RAID 6 que contienen datos.

Para crear una partición RAID 1:

1. Asegúrese de que los discos de las ranuras 0 y 1 funcionan correctamente.
2. Inicie el DL4000 Backup To Disk appliance (Servidor de copia de seguridad en disco DL4000).
3. Cuando se le solicite durante el inicio, pulse <Ctrl><R>.

   Se muestra la pantalla **PERC BIOS Configuration Utility (Utilidad de configuración del BIOSde PERC)**.
4. Resalte la controladora en la parte superior de la pestaña **VD Management (Administración de VD)** y pulse <F2>;a continuación, seleccione **Create New VD (Crear VD nuevo)**.

   NOTA: Si el VD RAID-1 OS VD ya existe, realice una inicialización rápida del VD RAID-1 OS.
5. En la página **Virtual Disk Management (Administración de disco virtual)**, seleccione RAID 1 para RAID Level (Nivel de RAID).
6. Seleccione ambos discos en la casilla **Physical Disks (Discos físicos)**.
7. Introduzca un nombre de disco virtual (VD), como por ejemplo, "OS", que identifique el disco virtual como el que contiene el sistema operativo (OS).
8. Presione <Tab> para desplazar el cursor hasta Inicializar y presione <Intro>.

   NOTA: La inicialización que se lleva a cabo en esta fase es una inicialización rápida.
9. Haga clic en **OK (Aceptar)** para finalizar la selección o pulse <Ctrl><N> dos veces.

Se abrirá la página **Ctrl Mgt (Adm. ctrl.)**.

10. Vaya al campo **Select boot device (Seleccionar dispositivo de inicio)** y seleccione el disco virtual que contiene el sistema operativo.

    La capacidad de este disco es de aproximadamente 278 GB.

11. Seleccione **Apply (Aplicar)** y presione <Intro>.
12. Salga de la utilidad **PERC BIOS Configuration (Configuración del BIOS de PERC)** y presionee <Ctrl><Alt><Del> para reiniciar el sistema.

Instalación del sistema operativo

Utilice la utilidad Unified Server Configurator - Lifecycle Controller Enabled (Configurador de servidor unificado: Controladora de ciclo de vida habilitada; USC-LCE) en el sistema DL4000 para recuperar el sistema operativo:

1. Tenga a mano los soportes multimedia de instalación del sistema operativo.
2. Asegúrese de que dispone de una unidad desde la que ejecutar los medios.

   Puede utilizar una unidad óptica iDRAC o un dispositivo de medios virtuales. Los medios virtuales se admiten a través de iDRAC. Para obtener más información sobre la configuración de medios virtuales a través de iDRAC, consulte la User Guide for your system's iDRAC device (Guía de usuario del dispositivo iDRAC de su sistema).

   Si el medio de instalación está dañado o no puede leerse, es posible que USC no pueda detectar la presencia de una unidad óptica compatible. En este caso, puede recibir un mensaje de error que indique que no hay ninguna unidad óptica disponible. Si el medio no es válido (si es el CD o DVD incorrecto, por ejemplo), se muestra un mensaje de error para solicitarle introducir el medio de instalación correcto.
3. Para iniciar USC, inicie el sistema y presione la tecla <F10> en los 10 segundos siguientes a la aparición del logotipo de Dell.
4. Haga clic en **OS Deployment (Implementación del SO)** en el panel izquierdo.
5. Haga clic en **Deploy OS (Implementación del SO)** en el panel derecho.
6. Seleccione el sistema operativo correspondiente y haga clic en **Next (Siguiente)**.

   USC extrae los controladores necesarios para el sistema operativo seleccionado. Los controladores se extraen a una unidad USB interna denominada OEMDRV.

   NOTA: El proceso de extracción de los controladores puede tardar varios minutos.

   NOTA: Todos los controladores copiados por el OS Deployment wizard (Asistente de implementación del SO) se eliminan transcurridas 18 horas. Debe completar la instalación del sistema operativo en el plazo de 18 horas para que los controladores copiados estén disponibles. Para eliminar los controladores antes de que transcurra el periodo de 18 horas, reinicie el sistema y presione la tecla <F10> para volver acceder a USC. El uso de la tecla <F10> para cancelar la instalación del sistema operativo o volver a acceder a USC después de reiniciar elimina los controladores durante el periodo de 18 horas.
7. Una vez extraídos los controladores, USC le solicitará que inserte el medio de instalación del sistema operativo. Inserte el medio de instalación.

   NOTA: Al instalar el sistema operativo Microsoft Windows, los controladores extraídos se instalarán automáticamente durante la instalación del sistema operativo.

Ejecución de la Recovery and Update Utility (Utilidad de actualización y recuperación)

Para ejecutar la Recovery and Update Utility (Utilidad de actualización y recuperación):

1. Descargue **Recovery and Update Utility (Utilidad de actualización y recuperación)** desde **dell.com/support**.
2. Copie la utilidad en el escritorio del DL4000 Backup to Disk Appliance (Appliance de copia de seguridad en disco DL4000) y extraiga los archivos.
3. Haga doble clic en **Launch-RUU (Abrir-RUU)**.
4. Cuando se le solicite, haga clic en **Yes (Sí)** para aceptar que no está ejecutando ninguno de los procesos enumerados.
5. Haga clic en **Start (Inicio)** cuando se muestre la pantalla de la **Recovery and update utility (Utilidad de actualización y recuperación)**.
6. Cuando se le solicite reiniciar, haga clic en **OK (Aceptar)**.

   Las versiones de funciones y características de Windows Server, ASP .NET MVC3, proveedor de LSI, aplicaciones DL, OpenManage Server Administrator y del software AppAssure Core se instalan como parte de la utilidad de recuperación y actualización.
7. Reinicie el sistema si se le solicita de nuevo.
8. Haga clic en **Proceed (Continuar)** cuando todos los servicios y aplicaciones estén instalados.

   Se iniciará el asistente de **AppAssure Appliance Recovery (Recuperación del servidor AppAssure)**.
9. Complete los pasos de la fase **Collecting Information and Configuring (Recopilación de información y configuración)** del AppAssure Appliance Recovery Wizard (Asistente de recuperación del servidor AppAssure) y, a continuación, haga clic en **Next (Siguiente)**.

   Se iniciará la fase **Disk Recovery (Recuperación de disco)**.
10. Haga clic en **Next (siguiente)** cuando se muestre el aviso sobre el apagado de los servicios de AppAssure.

    Se restauran los discos virtuales para los repositorios y cualquier máquina en espera virtual y se reinician los servicios de AppAssure. La recuperación finaliza.

8

Cómo cambiar el nombre del host manualmente

Se recomienda seleccionar un nombre del host durante la configuración inicial del DL4000 Backup to Disk Appliance (Servidor de copia de seguridad en disco DL4000). Si cambia el nombre del host posteriormente mediante las **Windows System Properties (Propiedades del sistema Windows)**, debe realizar los pasos siguientes manualmente para garantizar que el nuevo nombre del host entre en vigor y el servidor funcione correctamente:

1. Detener el servicio AppAssure Core
2. Eliminar los certificados del servidor AppAssure
3. Eliminar el servidor del Core y las claves de registro
4. Cambiar el nombre de visualización en AppAssure
5. Actualizar los sitios de confianza en Internet Explorer

Detención del servicio de Core

Para detener los servicios de AppAssure Core:

1. Abra **Windows Server Manager**.
2. En el árbol situado a la izquierda, seleccione **Configuration (Configuración) → Services (Servicios).**
3. Haga clic con el botón derecho del mouse en **AppAssure Core Service (Servicio de Appassure Core)** y seleccione **Stop (Detener)**.

Eliminación de certificados del servidor

Eliminar certificados del servidor AppAssure:

1. Abra una interfaz de línea de comandos.
2. Escriba **Certmgr** y presione <Intro>.
3. En la ventana **Certificate Manager (Administrador de certificados)**, seleccione **Trusted Root Certification Authorities (Autoridades de certificación raíz de confianza) → Certificates (Certificados).**
4. Elimine cualquier certificado para el que la columna **Issue To (Emitido para)** muestre el nombre del host antiguo y la columna **Intended Purpose (Propósito previsto)** muestre **Server Authentication (Autentificación del servidor)**.

Eliminación del servidor del Core y de las claves de registro

Para eliminar el servidor del Core y las claves de registro:

1. Abra una interfaz de línea de comandos.
2. Escriba **regedit** y presione <Intro> para abrir el editor de registros.
3. En el árbol, vaya a **HKEY_LOCAL_MACHINE** → **SOFTWARE** → **AppRecovery** y abra el directorio del Core.
4. Elimine los directorios **webServer** y **serviceHost**.

Inicio de Core con el nuevo nombre de host

Para iniciar el Core con el nuevo nombre del host creado manualmente:

1. Inicie los servicios de AppAssure Core.
2. En el escritorio, haga clic con el botón derecho del mouse en el icono **AppAssure 5 Core** y, a continuación, haga clic en **Properties (Propiedades)**.
3. Reemplace el nombre del servidor antiguo por el nuevo `<server name:8006>`.

   Por ejemplo, **https://<servername:8006/apprecovery/admin/Core**.
4. Haga clic en **OK (Aceptar)** y, después, inicie la AppAssure 5 Core Console mediante el icono **AppAssure 5 Core**.

Cómo cambiar el nombre de visualización

Para cambiar el nombre de visualización:

1. Inicie sesión en la **AppAssure Console** como administrador.
2. Seleccione la pestaña **Configuration (Configuración)** y, a continuación, haga clic en el botón de cambio en la barra **General**.
3. Introduzca el nuevo **Display Name (Nombre de visualización)** y haga clic en **OK (Aceptar)**.

Actualización de los sitios de confianza en Internet Explorer

Para actualizar los sitios de confianza en Internet Explorer:

1. Abra Internet Explorer.
2. Si **File (Archivo)**, **Edit View (Editar vista)** y demás menús no aparecen, presione <F10>.
3. Haga clic en el menú **Tools (Herramientas)** y seleccione **Internet Options (Opciones de Internet)**.
4. En la ventana **Internet Options (Opciones de Internet)**, haga clic en la pestaña **Security (Seguridad)**.
5. Haga clic en **Trusted Sites (Sitios de confianza)** y, a continuación, haga clic en **Sites (Sitios)**.
6. En **Add this website to the zone (Agregar este sitio web a la zona)**, introduzca **https://[Display Name]**, usando el nuevo nombre que haya proporcionado para el nombre de visualización.
7. Haga clic en **Add (Agregar)**.
8. En **Add this website to the zone (Agregar este sitio web a la zona)**, escriba **about:blank**.

9. Haga clic en **Add (Agregar)**.
10. Haga clic en **Close (Cerrar)** y, a continuación, en **OK (Aceptar)**.

9

Apéndice A — Secuencias de comandos

Acerca de las secuencias de comandos de PowerShell

Windows PowerShell es un entorno conectado a Microsoft .NET Framework diseñado para la automatización administrativa. AppAssure 5 incluye kits de desarrollo de software (SDK) completos para secuencias de comandos de PowerShell que permite a los administradores automatizar la administración de los recursos de AppAssure 5 mediante la ejecución de comandos a través de secuencias de comandos.

Permite a los usuarios administrativos ejecutar secuencias de comandos de PowerShell proporcionados por el usuario en repeticiones designadas. Por ejemplo, antes o después de una instantánea, comprobaciones de conectividad y capacidad de montaje, etc. Los administradores pueden ejecutar secuencias de comandos tanto desde el AppAssure 5 Core como desde el Agent. Las secuencias de comandos pueden aceptar parámetros y la salida de una secuencia de comandos se escribe en los archivos de registro del Core y el Agent.

NOTA: Para los trabajos nocturnos, debe conservar un archivo de secuencia de comandos y el parámetro de entrada JobType para distinguir entre los trabajos nocturnos.

Los archivos de secuencia de comandos se encuentran en la carpeta **%ALLUSERSPROFILE%\AppRecovery\Scripts**:

- En Windows 7, la ruta de aceeso para localizar la carpeta **%ALLUSERSPROFILE%** es: **C:\ProgramData**.
- En Windows 2003, la ruta de acceso para localizar la carpeta es: **Documents and Settings\All Users\Application Data**.

NOTA: Windows PowerShell es necesario y debe estar instalado y configurado antes de usar y ejecutar secuencias de comandos de AppAssure 5.

Requisitos previos para secuencias de comandos de PowerShell

Para poder utilizar y ejecutar secuencias de comandos de PowerShell para AppAssure 5, debe tener instalado Windows PowerShell 2.0.

NOTA: Asegúrese de ubicar el archivo **powershell.exe.config** en el directorio de inicio de PowerShell. Por ejemplo, **C:\WindowsPowerShell\powershell.exe**.

powershell.exe.config

```
<?xml version="1.0"?>
<configuration>
        <startup useLegacyV2RuntimeActivationPolicy="true">
        <supportedRuntime version="v4.0.30319"/>
<supportedRuntime version="v2.0.50727"/>
</startup>
</configuration>
```

Pruebas de secuencias de comandos

Si desea probar las secuencias de comandos que tiene pensado ejecutar, podrá hacerlo utilizando el editor gráfico de PowerShell, **powershell_is**. También es necesario que agregue el archivo de configuración, **powershell_ise.exe.config**, a la misma carpeta del archivo de configuración, **powershell.exe.config**.

NOTA: El archivo de configuración, **powershell_ise.exe.config** debe tener el mismo contenido que el archivo **powershell.exe.config**.

PRECAUCIÓN: Si la secuencia de comandos previa o posterior de PowerShell falla, el trabajo también fallará.

Parámetros de entrada

Todos los parámetros de entrada disponibles se utilizan en secuencias de comandos de ejemplo. Los parámetros se describen en las siguientes tablas.

NOTA: Los archivos de secuencias de comandos deben tener el mismo nombre que los archivos de secuencias de comandos de ejemplo.

Tabla 4. AgentProtectionStorageConfiguration (namespace Replay.Common.Contracts.Agents)

Método	Descripción
`public Guid RepositoryId { get; set; }`	Obtiene o establece la Id. del repositorio en el que se almacenan los puntos de recuperación de este Agent.
`public string EncryptionKeyId { get; set; }`	Obtiene o establece la Id. de la clave de cifrado para los puntos de recuperación de este Agent. Una secuencia de comandos vacía significa que no existe cifrado.

Tabla 5. AgentTransferConfiguration (namespace Replay.Common.Contracts.Transfer)

Método	Descripción
`public uint MaxConcurrentStreams { get; set; }`	Obtiene o establece el número máximo de conexiones TCP simultáneas que el Core establece para el Agent, para la transferencia de datos.
`public uint MaxTransferQueueDepth { get; set; }`	Cuando se lee un intervalo de bloques desde una transmisión de transferencia, el intervalo se ubica en una cola de productor o consumidor, donde un subproceso consumidor realiza la lectura y posterior escritura en el objeto de época. Si el repositorio escribe a un ritmo más lento que el ritmo de escritura de la red, esta cola se llenará. El punto en el que la cola se llena y se detiene la lectura es la profundidad de cola de transferencia máxima.

Método	Descripción
`public uint MaxConcurrentWrites { get; set; }`	Obtiene o establece el número máximo de operaciones de escritura de bloque que pueden estar pendientes en una época en cualquier momento. Si se reciben bloques adicionales cuando se alcanza esta cantidad de escrituras de bloque pendientes, se ignoran los bloques adicionales hasta que finalice una de las escrituras pendientes.
`public ulong MaxSegmentSize { get; set; }`	Obtiene o establece el número máximo de bloques contiguos que se pueden transferir en una solicitud individual. En función de las pruebas, pueden ser adecuados valores más altos o más bajos.
`public Priority Priority { get; set; }`	Obtiene o establece la prioridad para la solicitud de transferencia.
`public int MaxRetries { get; set; }`	Obtiene o establece el número máximo de reintentos para una transferencia errónea antes de que se considere como errónea.
`public Guid ProviderId{ get; set; }`	Obtiene o establece la GUID del proveedor VSS que se utilizará para las instantáneas en este host. Los administradores aceptan normalmente el valor predeterminado.
`public Collection<ExcludedWriter>ExcludedWriterIds { get; set; }`	Obtiene o establece la recopilación de las Id. de escritores VSS, que se excluyen de esta instantánea. La Id. de escritor se obtiene a partir del nombre del mismo. Este nombre solo se utiliza para fines de documentación y no es necesario que coincida exactamente con el nombre del escritor.
`public ushort TransferDataServerPort { get; set; }`	Obtiene o establece un valor que contiene el puerto TCP en el que aceptar conexiones desde el Core para la transferencia actual de datos desde el Agent hasta el Core. El Agent intenta escuchar en este puerto, aunque si el puerto está en uso, el Agent puede utilizar un puerto diferente en su lugar. El Core utiliza el número de puerto especificado en las propiedades `BlockHashesUri` y `BlockDataUri` del objeto `VolumeSnapshotInfo` para cada volumen dañado.
`public TimeSpan SnapshotTimeout { get; set; }`	Obtiene o establece el tiempo de espera para que se complete una operación de instantánea de VSS, antes de abandonar y considerar que ha superado el tiempo de espera máximo.

Método	Descripción
`public TimeSpan TransferTimeout { get; set; }`	Obtiene o establece el tiempo de espera para contacto posterior desde el Core antes de abandonar la instantánea.
`public TimeSpan NetworkReadTimeout { get; set; }`	Obtiene o establece el tiempo de espera para las operaciones de lectura de red relacionadas con esta transferencia.
`public TimeSpan NetworkWriteTimeout { get; set; }`	Obtiene o establece el tiempo de espera para las operaciones de escritura de red relacionadas con esta transferencia.

Tabla 6. BackgroundJobRequest (namespace Replay.Core.Contracts.BackgroundJobs)

Método	Descripción
`public Guid AgentId { get; set; }`	Obtiene o establece la Id. de Agent.
`public bool IsNightlyJob { get; set; }`	Obtiene o establece el valor indicando si el trabajo en segundo plano es un trabajo nocturno.
`public virtual bool InvolvesAgentId(Guid agentId)`	Determina el valor indicando si el Agent concreto está implicado en un trabajo.

ChecksumCheckJobRequest (namespace Replay.Core.Contracts.Exchange.ChecksumChecks)

Hereda sus valores del parámetro, `DatabaseCheckJobRequestBase`.

DatabaseCheckJobRequestBase (namespace Replay.Core.Contracts.Exchange)

Hereda sus valores del parámetro, `BackgroundJobRequest`.

ExportJobRequest (namespace Replay.Core.Contracts.Export)

Hereda sus valores del parámetro, `BackgroundJobRequest`.

Método	Descripción
`public uint RamInMegabytes { get; set; }`	Obtiene o establece el tamaño de memoria para la VM exportada. Se establece en cero (0) para utilizar el tamaño de memoria de la máquina de origen.
`public VirtualMachineLocation Location { get; set; }`	Obtiene o establece la ubicación de destino para esta exportación. Se trata de una clase base abstracta.
`public VolumeImageIdsCollection VolumeImageIds { get; private set; }`	Obtiene o establece las imágenes de volumen a incluir en la exportación de la VM.
`public ExportJobPriority Priority { get; set; }`	Obtiene o establece la prioridad para la solicitud de exportación.

NightlyAttachabilityJobRequest (namespace Replay.Core.Contracts.Sql)

Hereda sus valores del parámetro, `BackgroundJobRequest`.

RollupJobRequest (namespace Replay.Core.Contracts.Rollup)

Hereda sus valores del parámetro, `BackgroundJobRequest`.

TakeSnapshotResponse (namespace Replay.Agent.Contracts.Transfer)

Método	Descripción
`public Guid SnapshotSetId { get; set; }`	Obtiene o establece el GUID asignado por VSS a esta instantánea.
`public VolumeSnapshotInfoDictionary VolumeSnapshots { get; set; }`	Obtiene o establece la recopilación de información de instantánea para cada volumen incluido en el retén.

TransferJobRequest (namespace Replay.Core.Contracts.Transfer)

Hereda sus valores del parámetro, `BackgroundJobRequest`.

Método	Descripción
`public VolumeNameCollection VolumeNames { get; set; }`	Obtiene o establece la recopilación de los nombres de volumen para transferencia.
`public ShadowCopyType ShadowCopyType { get; set; }`	Obtiene o establece el tipo de copia para transferencia. Valores disponibles: `Unknown`, `Copy` y `Full`.
`Public AgentTransferConfiguration TransferConfiguration { get; set; }`	Obtiene o establece la configuración de transferencia.
`public AgentProtectionStorageConfiguration StorageConfiguration { get; set; }`	Obtiene o establece la configuración de almacenamiento.
`public string Key { get; set; }`	Genera una clave pseudoaleatoria (aunque no criptográficamente segura) que se puede utilizar como contraseña de un solo uso para autenticar solicitudes de transferencia.
`public bool ForceBaseImage { get; set; }`	Obtiene o establece el valor que indica si la imagen base se ha forzado o no.
`public bool IsLogTruncation { get; set; }`	Obtiene o establece el valor que indica si el trabajo es un truncamiento de registro o no.

Tabla 7. TransferPostscriptParameter (namespace Replay.Common.Contracts.PowerShellExecution)

Método	Descripción
`public VolumeNameCollection VolumeNames { get; set; }`	Obtiene o establece la recopilación de los nombres de volumen para transferencia.
`public ShadowCopyType ShadowCopyType { get; set; }`	Obtiene o establece el tipo de copia para transferencia. Valores disponibles: `Unknown`, `Copy` y `Full`.
`public AgentTransferConfiguration TransferConfiguration { get; set; }`	Obtiene o establece la configuración de transferencia.
`public AgentProtectionStorageConfiguration StorageConfiguration { get; set; }`	Obtiene o establece la configuración de almacenamiento.
`public string Key { get; set; }`	Genera una clave pseudoaleatoria (aunque no criptográficamente segura) que se puede utilizar como contraseña de un solo uso para autenticar solicitudes de transferencia.
`public bool ForceBaseImage { get; set; }`	Obtiene o establece el valor que indica si la imagen de base se ha forzado o no.
`public bool IsLogTruncation { get; set; }`	Obtiene o establece el valor que indica si el trabajo es un truncamiento de registro.
`public uint LatestEpochSeenByCore { get; set; }`	Obtiene o establece el valor de época más reciente.
`public Guid SnapshotSetId { get; set; }`	Obtiene o establece el GUID asignado por VSS a esta instantánea.
`public VolumeSnapshotInfoDictionary VolumeSnapshots { get; set; }`	Obtiene o establece la recopilación de información de instantánea para cada volumen incluido en el retén.

Tabla 8. TransferPrescriptParameter (namespace Replay.Common.Contracts.PowerShellExecution)

Método	Descripción
`public VolumeNameCollection VolumeNames { get; set; }`	Obtiene o establece la recopilación de los nombres de volumen para transferencia.
`public ShadowCopyType ShadowCopyType { get; set; }`	Obtiene o establece el tipo de copia para transferencia. Valores disponibles: `Unknown`, `Copy` y `Full`.
`public AgentTransferConfiguration TransferConfiguration { get; set; }`	Obtiene o establece la configuración de transferencia.
`public AgentProtectionStorageConfiguration StorageConfiguration { get; set; }`	Obtiene o establece la configuración de almacenamiento.

Método	Descripción
`public string Key { get; set;}`	Genera una clave pseudoaleatoria (aunque no criptográficamente segura) que se puede utilizar como contraseña de un solo uso para autenticar solicitudes de transferencia.
`public bool ForceBaseImage { get; set; }`	Obtiene o establece el valor que indica si la imagen de base se ha forzado o no.
`public bool IsLogTruncation { get; set; }`	Obtiene o establece el valor que indica si el trabajo es un truncamiento de registro.
`public uint LatestEpochSeenByCore { get; set; }`	Obtiene o establece el valor de época más reciente.

Tabla 9. VirtualMachineLocation (namespace Replay.Common.Contracts.Virtualization)

Método	Descripción
`public string Description { get; set;}`	Obtiene o establece una descripción de esta ubicación que el usuario puede entender.
`public string Method { get; set;}`	Obtiene o establece el nombre de la VM.

VolumeImageIdsCollection (namespace Replay.Core.Contracts.RecoveryPoints)

Hereda sus valores del parámetro, `System.Collections.ObjectModel.Collection<string>`.

Tabla 10. VolumeName (namespace Replay.Common.Contracts.Metadata.Storage)

Método	Descripción
`public string GuidName { get; set;}`	Obtiene o establece la Id. del volumen.
`public string DisplayName { get; set;}`	Obtiene o establece el nombre del volumen.
`public string UrlEncode()`	Obtiene una versión codificada de la URL del nombre que se puede pasar de forma limpia en una URL. **NOTA:** Existe un problema conocido en .NET 4.0 WCF (**https://connect.microsoft.com/VisualStudio/ feedback/ ViewFeedback.aspx?FeedbackID=413312**), que impide el funcionamiento correcto de caracteres de escape de ruta de acceso en una plantilla URI. Debido a que un nombre de volumen contiene '\' y '?', debe sustituir los caracteres especiales '\' y '?' por otros caracteres especiales.
`public string GetMountName()`	Devuelve un nombre para este volumen, que es válido para montar la imagen del volumen en la misma carpeta.

VolumeNameCollection (namespace Replay.Common.Contracts.Metadata.Storage)

Hereda sus valores del parámetro, `System.Collections.ObjectModel.Collection<VolumeName>`.

Método	Descripción
`public override bool Equals(object obj)`	Determina si la instancia y un objeto especificado, que también debe ser un objeto `VolumeNameCollection`, tienen el mismo valor. (Reemplaza a `Object.Equals(Object)`.)
`public override int GetHashCode()`	Devuelve el código hash para este `VolumeNameCollection`. (Suprime `Object.GetHashCode()`.)

Tabla 11. VolumeSnapshotInfo (namesapce Replay.Common.Contracts.Transfer)

Método	Descripción
`public Uri BlockHashesUri { get; set;}`	Obtiene o establece el URI en el que los hashes MD5 de los bloques de volumen se pueden leer.
`public Uri BlockDataUri { get; set;}`	Obtiene o establece el URI en el que los bloques de datos de volumen se pueden leer.

VolumeSnapshotInfoDictionary (namespace Replay.Common.Contracts.Transfer)

Hereda sus valores del parámetro, `System.Collections.Generic.Dictionary<VolumeName, VolumeSnapshotInfo>`.

Pretransferscript.ps1

PreTransferScript se ejecuta en el lado del Agent antes de transferir una instantánea.

```
# receiving parameter from transfer job
param([object]$TransferPrescriptParameter)

# building path to Agent's Common.Contracts.dll and loading this assembly
$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM = $regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall
\AppRecovery Agent 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal) | out-null

# Converting input parameter into specific object
$TransferPrescriptParameterObject = $TransferPrescriptParameter -as
[Replay.Common.Contracts.PowerShellExecution.TransferPrescriptParameter];
# Working with input object. All echo's are logged
if($TransferPrescriptParameterObject -eq $null) {
        echo 'TransferPrescriptParameterObject parameter is null'
}
else {
        echo
'TransferConfiguration:'$TransferPrescriptParameterObject.TransferConfiguration

        echo 'StorageConfiguration:'
```

```
$TransferPrescriptParameterObject.StorageConfiguration
}
```

Posttransferscript.ps1

PostTransferScript se ejecuta en el lado del Agent después de transferir una instantánea.

```
 # receiving parameter from transfer job
param([object] $TransferPostscriptParameter)


# building path to Agent's Common.Contracts.dll and loading this assembly

$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM = $regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall
\AppRecovery Agent 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal) | out-null


# Converting input parameter into specific object

$TransferPostscriptParameterObject = $TransferPostscriptParameter -as
[Replay.Common.Contracts.PowerShellExecution.TransferPostscriptParameter];


# Working with input object. All echo's are logged
if($TransferPostscriptParameterObject -eq $null) {
        echo 'TransferPostscriptParameterObject parameter is null'
}
else {
echo 'VolumeNames:' $TransferPostscriptParameterObject.VolumeNames
                echo 'ShadowCopyType:'
$TransferPostscriptParameterObject.ShadowCopyType
        echo 'ForceBaseImage:'
$TransferPostscriptParameterObject.ForceBaseImage                    echo
'IsLogTruncation:' $TransferPostscriptParameterObject.IsLogTruncation
}
```

Preexportscript.ps1

PreExportScript se ejecuta en el lado del Core antes de la exportación de cualquier trabajo.

```
# receiving parameter from export job

param([object]$ExportJobRequest)

# building path to Core's Common.Contracts.dll and loading this assembly

$regLM = [Microsoft.Win32.Registry]::LocalMachine$regLM =
$regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall
\AppRecovery Core 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'CoreService\Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal) | out-null

# Converting input parameter into specific object

$ExportJobRequestObject = $ExportJobRequest -as
[Replay.Core.Contracts.Export.ExportJobRequest]

# Working with input object. All echo's are logged
```

```
if($ExportJobRequestObject -eq $null) {
                echo 'ExportJobRequestObject parameter is null'
}
else {
                echo 'Location:' $ExportJobRequestObject.Location
                echo 'Priority:' $ExportJobRequestObject.StorageConfiguration
}
```

Postexportscript.ps1

PostExportScript se ejecuta en el lado del Core, después de la exportación de cualquier trabajo.

NOTA: No existen parámetros de entrada para **PostExportScript** cuando se utiliza para su ejecución una vez en el Agent exportado tras el arranque inicial. El Agent normal contiene esta secuencia de comandos en la carpeta de secuencias de comandos de PowerShell como **PostExportScript.ps1**.

```
# receiving parameter from export job

param([object]$ExportJobRequest)

# building path to Core's Common.Contracts.dll and loading this assembly
$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM = $regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall
\AppRecovery Core 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'CoreService\Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal) | out-null
$regVal2 = $regLM.GetValue('InstallLocation')
$regVal2 = $regVal2 + 'CoreService\Common.Contracts.dll'

# Converting input parameter into specific object

$ExportJobRequestObject = $ExportJobRequest -as
[Replay.Core.Contracts.Export.ExportJobRequest]

# Working with input object. All echo's are logged

if($ExportJobRequestObject -eq $null) {
            echo 'ExportJobRequestObject parameter is null'
}
else {
            echo 'VolumeImageIds:' $ExportJobRequestObject.VolumeImageIds
            echo 'RamInMegabytes:' $ExportJobRequestObject.RamInMegabytes
}
```

Prenightlyjobscript.ps1

PreNightlyJobScript se ejecuta antes de cada trabajo nocturno en el lado del Core. Incluye el parámetro **$JobClassName**, que ayuda a tramitar estos trabajos secundarios de manera independiente.

```
 # receiving parameters from Nightlyjob
param([System.String]$JobClassMethod , [object]
$NightlyAttachabilityJobRequest,
[object]$RollupJobRequest, [object]$Agents, [object]$ChecksumCheckJobRequest,
[object]$TransferJobRequest, [int]$LatestEpochSeenByCore)

# building path to Core's Common.Contracts.dll and loading this assembly
$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM = $regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall
\AppRecovery Core 5')
$regVal = $regLM.GetValue('InstallLocation')
```

```
$regVal = $regVal + 'CoreService\Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal) | out-null

# Nightlyjob has four child jobs: NightlyAttachability Job, Rollup Job,
Checksum Check Job and Log  Truncation Job. All of them are triggering the
script, and $JobClassMethod (contain job name that calls the  script) helps to
handle those child jobs separately

switch ($JobClassMethod) {

# working with NightlyAttachability Job
        NightlyAttachabilityJob {
                $NightlyAttachabilityJobRequestObject =
$NightlyAttachabilityJobRequest -as
[Replay.Core.Contracts.Sql.NightlyAttachabilityJobRequest];

                echo 'Nightly Attachability job results:';
                if($NightlyAttachabilityJobRequestObject -eq $null) {
                        echo 'NightlyAttachabilityJobRequestObject parameter is
null';
                }

                else {
                                echo 'AgentId:'
$NightlyAttachabilityJobRequestObject.AgentId;
                                echo 'IsNightlyJob:'
$NightlyAttachabilityJobRequestObject.IsNightlyJob;
                }
                break;
}


# working with Rollup Job
RollupJob {
        $RollupJobRequestObject = $RollupJobRequest -as
[Replay.Core.Contracts.Rollup.RollupJobRequest];
        echo 'Rollup job results:';
        if($RollupJobRequestObject -eq $null) {
                echo 'RollupJobRequestObject parameter is null';
        }
        else {
                    echo 'SimultaneousJobsCount:'
$RollupJobRequestObject.SimultaneousJobsCount;
                    echo 'AgentId:' $RollupJobRequestObject.AgentId;
                    echo 'IsNightlyJob:' $RollupJobRequestObject.IsNightlyJob;
        }
        $AgentsCollection = $Agents -as
"System.Collections.Generic.List``1[System.Guid]"
        if($AgentsCollection -eq $null) {
            echo 'AgentsCollection parameter is null';
        }
        else {
                    echo 'Agents GUIDs:'
                    foreach ($a in $AgentsCollection) {
                        echo $a
                }
        }
        break;
}

# working with Checksum Check Job
        ChecksumCheckJob {
                $ChecksumCheckJobRequestObject = $ChecksumCheckJobRequest -as
```

```
[Replay.Core.Contracts.Exchange.ChecksumChecks.ChecksumCheckJobRequest];
                echo 'Exchange checksumcheck job results:';
                if($ChecksumCheckJobRequestObject -eq $null) {
                        echo 'ChecksumCheckJobRequestObject parameter is null';
                }
                else {
                                echo 'RecoveryPointId:'
$ChecksumCheckJobRequestObject.RecoveryPointId;
                                echo 'AgentId:'
$ChecksumCheckJobRequestObject.AgentId;
                                echo 'IsNightlyJob:'
$ChecksumCheckJobRequestObject.IsNightlyJob;
                }
                break;
}


# working with Log Truncation Job
        TransferJob {
                $TransferJobRequestObject = $TransferJobRequest -as
                [Replay.Core.Contracts.Transfer.TransferJobRequest];
        echo 'Transfer job results:';
        if($TransferJobRequestObject -eq $null) {
                echo 'TransferJobRequestObject parameter is null';
        }
        else {
                echo 'TransferConfiguration:'
$TransferJobRequestObject.TransferConfiguration;
                echo 'StorageConfiguration:'
$TransferJobRequestObject.StorageConfiguration;
        }
        echo 'LatestEpochSeenByCore:' $LatestEpochSeenByCore;
        break;
    }
}
```

Postnightlyjobscript.ps1

PostNightlyJobScript se ejecuta después de cada trabajo nocturno en el lado del Core. Tiene el parámetro **$JobClassName**, que ayuda a manejar dichos trabajos secundarios por separado.

```
 # receiving parameters from Nightlyjob
param([System.String]$JobClassMethod , [object]
$NightlyAttachabilityJobRequest,  [object]$RollupJobRequest, [object]$Agents,
[object]$ChecksumCheckJobRequest,  [object]$TransferJobRequest, [int]
$LatestEpochSeenByCore, [object]$TakeSnapshotResponse)

# building path to Core's Common.Contracts.dll and loading this assembly

$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM = $regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall
\AppRecovery Core 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'CoreService\Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal) | out-null
$regVal2 = $regLM.GetValue('InstallLocation')
$regVal2= $regVal2 + 'CoreService\Core.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal2) | out-null


# Nightlyjob has four child jobs: NightlyAttachability Job, Rollup Job,
Checksum Check Job and Log Truncation Job. All of them are triggering the
script, and $JobClassMethod (contain job name that calls the script) helps to
```

```
handle those child jobs separately

switch ($JobClassMethod) {


# working with NightlyAttachability Job

NightlyAttachabilityJob {
        $NightlyAttachabilityJobRequestObject = $NightlyAttachabilityJobRequest
-as
[Replay.Core.Contracts.Sql.NightlyAttachabilityJobRequest];
        echo 'Nightly Attachability job results:';
        if($NightlyAttachabilityJobRequestObject -eq $null) {
                echo 'NightlyAttachabilityJobRequestObject parameter is null';
        }
        else {
                echo 'AgentId:' $NightlyAttachabilityJobRequestObject.AgentId;
                echo 'IsNightlyJob:'
$NightlyAttachabilityJobRequestObject.IsNightlyJob;
        }
        break;
}


# working with Rollup Job

RollupJob {
        $RollupJobRequestObject = $RollupJobRequest -as
[Replay.Core.Contracts.Rollup.RollupJobRequest];
        echo 'Rollup job results:';
        if($RollupJobRequestObject -eq $null) {
                echo 'RollupJobRequestObject parameter is null';
        }
        else {
                echo 'SimultaneousJobsCount:'
$RollupJobRequestObject.SimultaneousJobsCount;
                echo 'AgentId:' $RollupJobRequestObject.AgentId;
                echo 'IsNightlyJob:' $RollupJobRequestObject.IsNightlyJob;
        }
        $AgentsCollection = $Agents -as
"System.Collections.Generic.List``1[System.Guid]"
        if($AgentsCollection -eq $null) {
                echo 'AgentsCollection parameter is null';
        }
        else {
                echo 'Agents GUIDs:'
                foreach ($a in $AgentsCollection) {
                echo $a
            }
        }
        break;
}


# working with Checksum Check Job
        ChecksumCheckJob {
                $ChecksumCheckJobRequestObject = $ChecksumCheckJobRequest -as
[Replay.Core.Contracts.Exchange.ChecksumChecks.ChecksumCheckJobRequest];
                echo 'Exchange checksumcheck job results:';
                if($ChecksumCheckJobRequestObject -eq $null) {
                        echo 'ChecksumCheckJobRequestObject parameter is null';
                }
                else {
                        echo 'RecoveryPointId:'
```

```
$ChecksumCheckJobRequestObject.RecoveryPointId;
                        echo 'AgentId:' $ChecksumCheckJobRequestObject.AgentId;
                        echo 'IsNightlyJob:'
$ChecksumCheckJobRequestObject.IsNightlyJob;
                }
        break;
    }


# working with Log Truncation Job
        TransferJob {
                $TransferJobRequestObject = $TransferJobRequest -as
[Replay.Core.Contracts.Transfer.TransferJobRequest];
                echo 'Transfer job results:';
                if($TransferJobRequestObject -eq $null) {
                        echo 'TransferJobRequestObject parameter is null';
                }
                else {
                        echo 'TransferConfiguration:'
$TransferJobRequestObject.TransferConfiguration;
                        echo 'StorageConfiguration:'
$TransferJobRequestObject.StorageConfiguration;
                }
                echo 'LatestEpochSeenByCore:' $LatestEpochSeenByCore;
                $TakeSnapshotResponseObject = $TakeSnapshotResponse -as
[Replay.Agent.Contracts.Transfer.TakeSnapshotResponse];
                if($TakeSnapshotResponseObject -eq $null) {
                        echo 'TakeSnapshotResponseObject parameter is null';
                }
                else {
                        echo 'ID of this transfer session:'
$TakeSnapshotResponseObject.Id;
                        echo 'Volumes:' $TakeSnapshotResponseObject.Volumes;
                }
                break;
        }
}
```

Secuencias de comandos de ejemplo

Las secuencias de comandos de ejemplo siguientes se proporcionan para ayudar a los usuarios administrativos en la ejecución de dichas secuencias de comandos de PowerShell.

Las secuencias de comandos de ejemplo incluyen:

- PreTransferScript.ps1
- PostTransferScript.ps1
- PreExportScript.ps1
- PostExportScript.ps1
- PreNightlyJobScript.ps1
- PostNightlyJobScript.ps1

10

Obtención de ayuda

Búsqueda de documentación

Existen enlaces directos a la documentación de AppAssure y del appliance DL4000 en la AppAssure 5 Core Console. Para acceder a los enlaces a la documentación, seleccione la pestaña **Appliance** y, después, haga clic en **Overall Status (Estado general)**. Los enlaces a la documentación se encuentran en la sección **Documentation (Documentación)**.

Búsqueda de actualizaciones de software

Existen enlaces directos a las actualizaciones de software de AppAssure y del servidor DL4000 en la AppAssure 5 Core Console. Para acceder a los enlaces de las actualizaciones de software, seleccione la pestaña **Appliance** y, después, haga clic en **Overall Status (Estado general)**. Los enlaces de las actualizaciones de software se encuentran en la sección **Documentation (Documentación)**.

Cómo ponerse en contacto con Dell

NOTA: Dell proporciona varias opciones de servicio y asistencia en línea y por teléfono. Si no tiene una conexión a Internet activa, puede encontrar información de contacto en su factura de compra, en su albarán de entrega, en su recibo o en el catálogo de productos Dell. La disponibilidad varía según el país y el producto y es posible que algunos de los servicios no estén disponibles en su área.

Si desea ponerse en contacto con Dell para tratar asuntos relacionados con las ventas, la asistencia técnica o el servicio al cliente:

1. Vaya a **dell.com/contactdell**.
2. Seleccione su país o región en el mapa mundial interactivo.
   Al seleccionar una región, se muestran los países para las regiones seleccionadas.
3. Seleccione el idioma apropiado bajo el país que haya seleccionado.
4. Seleccione la parte de su negocio.
   Se muestra la página de asistencia principal para la parte de negocio seleccionada.
5. Seleccione la opción adecuada según sus necesidades.

Comentarios sobre la documentación

Si tiene comentarios para este documento, escriba a **documentation_feedback@dell.com**. De forma alternativa, puede hacer clic en el enlace **Feedback (Comentarios)** en cualquiera de las páginas de documentación de Dell, rellenar el formulario y hacer clic en **Submit (Enviar)** para enviar sus comentarios.